Security issues

Security track record

Chamilo LMS has a great track record for fixing reported security issues, working together with security actors, publishing fixes prior to the official publication of the vulnerabilities on official sites.

So far, in the history of the project (since late 2009), all (but one) vulnerabilities have been fixed less than 120h (5 days) after they were reported to us, and the process of code revision by packagers before inclusion (no unchecked plugin) has always been followed, making it **the most secure open source e-learning platform** to date.

You can see a graphical representation of the reports and fixes here (with corresponding links to check details):
http://www.cvedetails.com/product/26528/Chamilo-Chamilo-Lms.html?vendor_id=12983
(navigate and check other LMSes to compare their security track record).

If you consider using another LMS, please (for your own sake) check its security track (sometimes, months can pass before fixes are provided publicly).

Check Secure_development_policy for more info.

Security flaws reporting procedure

If you have found a new security flaw in Chamilo, please send us an e-mail at security@chamilo.org and info@chamilo.org, including "Chamilo Vulnerability" in your topic line. We **will** respond quickly to these (usually within 24h), so if you don't receive an answer, please consider it might not have been received and send it again.
In the worst case, open an issue in this issues tracking system to call for our attention, but please do not publish the flaw until a patch has been developed.

Security flaws fixing procedure

Security matters to us. A lot. So when we receive a security flaw report, we will treat it very quickly (usually in a matter of 1 to 7 calendar days).
Our procedure is as follows:

1. we will report these issues in a private part of this issue tracker
2. one of us (developers) will be put in charge of providing a patch
3. the developer will publish the patch in our source code

Table of contents

repository (that's the first publication)

4. if relevant credits information has been sent to us, we will add this information to the code and the commit message to

Security flaws publication procedure

1. we will then prepare (and publish below) a full report and the corresponding patch to secure your platform. We will also provide the patch in the form of a zip to unzip into your Chamilo directory for the latest stable version
2. if you don't use the latest version, you will have to upgrade first **or** apply the patch by yourself in your version
3. if the security flaw has been passed to a security reporting authority, we will send them an e-mail

Issue '#30" - 2018-11-13 - Low risk - More XSS in agenda
Issue '#29' - 2018-10-06 - Moderate risk - XSS on registration page
Issue '#28' - 2018-10-05 - Low risk - XSS in agenda
Issue '#27' - 2018-08-06 - Moderate risk - Unauthenticated remote code execution
Issue '#26' - 2018-07-23 - Critical risk - Unauthenticated remote code execution
Issue '#25' - 2018-05-31 - Moderate risk - Data leak
Issue '#24' - 2018-04-09 - Low risk - Data leak
Issue '#23' - 2017-02-09 - Moderate risk - PHP File Upload
Issue '#22' - 2016-12-26 - Moderate risk - PHPMailer shell escaping flaw
Issue '#21' - 2016-07-15 - Moderate risk - User Input Sanitation
Issue '#20' - 2016-02-15 - Moderate risk - (messageId)
Issue '#19' - 2016-02-15 - Moderate risk - (messageId) Delete Post Vulnerability
Issue '#18' - 2015-05-02 - Low-Moderate risk - URL hijacking/spoofing
Issue '#17' - 2015-03-19 - Moderate risk - XSS & CSRF vulnerabilies
Issue '#16' - 2015-01-25 - High risk - SQL injection vulnerability in several queries
Issue '#15' - 2014-08-25 - Moderate-high risk - SQL injection in mySpace/users.php
Issue '#14' - 2014-06-18 - Moderate risk - XSS vulnerability in online editor
Issue '#13' - 2014-05-06 - Moderate risk - XSS vulnerability in user profile fields
Issue '#12' - 2014-03-05 - High risk - File injection through FCKEditor
Issue '#11' - 2013-12-09 - High risk - File injection through FCKEditor - CONFIRMED
Issue '#10' - 2013-11-06 - Moderate risk - SQL Injection in specific:
Issue '#9' - 2013-08-10 - Low risk - XSS in course title
Issue '#8' - 2013-03-04 - Moderate risk - Several moderate security flaws
Issue '#7' - 2012-07-16 - Moderate risk - Several moderate security flaws
Issue '#6" - 2011-06-15 - High risk - Several security flaws
Issue '#5' - 2011-01-31 - High risk - Filesystem traversal flaw
Issue '#4' - 2011-01-28 - High risk - Filesystem traversal flaw
Issue '#3' - 2010-12-09 - Low risk - Wiki and core weaknesses in specific configurations
Issue '#2' - 2010-09-29 - High risk - Course directory removal risk through tasks tool
Issue '#1' - 2010-08-02 - Wiki issues

.
.
.
.
.
.
.
.
.
.
.
.
.
.
.
.
.
.
.
.
.
.
.
.
.
.
.
.
.
.
.
.
.
.

Reported flaws

Issue "#95" - 2022-09-14 - High impact, Moderate risk - Authenticated Local file inclusion

Chamilo 1.11.16 allows big file uploads to copy/move local files out of the Chamilo directory.

Reported by: Eddie Zhang @ Willow Inc

Fix for Chamilo 1.11.6: https://github.com/chamilo/chamilo-lms/commit/b92887c6deb6a802607a071aecb519417e6024fc

Issue "#94" - 2022-09-06 - High impact, Moderate risk - Authenticated RCE via zipslip attack in file upload (CVE-2022-40407)

Chamilo uses the PclZip library since a very long time ago (so this affects many versions of Chamilo), and this library is vulnerabile to RCE via zipslip, a type of directory traversal. We highly recommend you update your Chamilo portal as soon as possible.

Reported by: Alex Mackey

- Fix for 1.11.* in environments with git/composer: just run "composer update"
- Fix for 1.11.* without support for git/composer:
    - Download the fixed PclZip library from here: https://github.com/chamilo/pclzip/releases/tag/v2.8.5 (.zip or .tar.gz, your choice)
    - Uncompress
    - Copy pclzip.lib.php to [your-chamilo-folder]/vendor/chamilo/pclzip/pclzip.lib.php
    - Done
- Fix for 1.10.* and earlier (note: also **please** update to 1.11)
    - Download the fixed PclZip library from here: https://github.com/chamilo/pclzip/releases/tag/v2.8.5 (.zip or .tar.gz, your choice)
    - Uncompress
    - Copy pclzip.lib.php to [your-chamilo-folder]/main/inc/lib/pclzip/pclzip.lib.php
    - Done

Issue "#93" - 2022-03-01 - High impact, Low risk - SSRF and Phar Deserialization vulnerability that lead to remote code execution

Chamilo uses the mPDF/Mpdf library to convert HTML to PDF. This can be abused by people able to edit the HTML (so with edition permissions) to trigger a Remote Code Execution vulnerability.
This probably affects all 1.11.* versions.

Reported by: Anna Violet

Fix for 1.11.16:
https://github.com/chamilo/chamilo-lms/commit/640ba55e6c50973e5771969ad9eee71e57024f5c
https://github.com/chamilo/chamilo-lms/commit/935f037972e8e465f51a3dcc56a69d9dcd37acd0
It is necessary to execute the "composer update" command after the update, to upgrade Mpdf from v6 to v8 (which contains complementary fixes).

Risk "R#1" - 2022-02-16 - Low impact, Low risk - XSS Vulnerability in SVG files

This is classified as a risk, not a classical vulnerability, because we believe there are enough conditions and features in Chamilo to mitigate or remove this issue.
Researcher @AggressiveUser reported that the documents tool (at least) in Chamilo was vulnerable to XSS embedded in SVG (see https://research.securitum.com/do-you-allow-to-load-svg-files-you-have-xss/ for example).

This is true: we **do** allow SVG files to be uploaded. We do **not** filter SVG content, and SVG files (or strings) can include JavaScript, and a browser, when interpreting SVG, will automatically execute whatever JS code this SVG file requests to be executed.

However, we **do** want to offer the possibility for teachers to be able to use the SVG format, and students, under teachers' supervision, to use it as well. SVG has unique qualities in terms of visual quality. It is perfect to present concepts in both an "extremely small" and "extremely large" view. Ideal for detailed schematics, for example. Ideal for education.

Filtering the JS code inside SVG is very tricky, as JS is allowed as part of SVG and, when present, is usually used to animate the SVG. We have looked for, but haven't found, any Open Source library that would allow to do this safely from PHP.

This puts us in a delicate situation, but we believe the following elements are sufficient to cover most, if not all, cases of SVG/XSS attack incidents.

- SVG can be used as uploaded files or inline SVG, embedded in HTML. We allow teachers and students to upload files and edit HTML files, and even create SVG files through an online tool, but all accesses to these tools are relatively limited.
- Editing SVG files through the online tool (SVGEdit) is only allowed to teachers or users with higher privileges than teachers, or in the case of the documents tool being shared through a users group.
- Uploading SVG files is allowed to students in several places (message attachments, wiki, dropbox, assignments), but the only places where these can be seen as SVG (and not as an uninterpreted attachment) are the forum and, if in groups, the document tool. The first tools are not affected by this SVG vulnerability because they only offer files as attachments. Final users could be affected only if they downloaded the files and then uploaded them to a web application, or if the opened it in a browser locally (which would be a very rare event and shouldn't have much impact). The document and forum tools will show the images and, as such, represent a risk, but also require the users to be identified on the platform. As such, we believe the risk is considerably reduced.
- Adding SVG inside the source of an HTML document is also bound to a user authentication, so an attack of this kind could be traced back to the original user.
- Viewing documents from the course require you to either be a student subscribed to the course, or requires the course to have been set as "public", which can only be done by a user with teacher privileges or above. Usually, courses set as "public" are only ever edited by teachers, so again... risk highly reduced. Other parts of the application which allow you to see images are either not editable by students or require authentication to access them. Risk highly reduced.
- File extensions can be filtered through blacklist or whitelist in the administration, so uploading SVGs can be prevented (editing HTML and creating SVG diagrams do not follow this rule, though).
- The SVG Editor in the documents tool can be disabled from the administration options.
- JS inside an inline SVG inside an HTML document will be filtered by the HTMLPurifier filter on HTML for non-teacher users (for teachers too, unless the course_introduction_html_strict_filtering setting has been turned off)
- Chamilo admins with SFTP or SSH access have the possibility to add Content Security Policy settings to configuration.php, as can be seen here https://github.com/chamilo/chamilo-lms/blob/1.11.x/main/install/configuration.dist.php#L559 and here https://github.com/chamilo/chamilo-lms/blob/1.11.x/main/install/configuration.dist.php#L588

For all these reasons combined, we believe it is acceptable to not prevent the upload of SVG file, in the context of the educational purpose of Chamilo, and in the context of the many options that exist to mitigate that risk.

We are incredibly thankful to researcher @AggressiveUser for having reported this issue, though, as it enabled us to grow conscious of the issue, and will allow us to better design Chamilo in the future, to put mechanisms in place that will better control the types of contents available for teachers to use in their courses.

Issue "#92" - 2021-11-12 - Low impact, Low risk - XSS Vulnerability in jCapture plugin (CVE-2021-43687)

A XSS Vulnerability in a parameter printed in a form by the jCapture plugin (a plugin seldom used in the documents tool to grab screencasts through a Java Applet).

Reported by: Feras AL-KASSAR (SAP) in the context of the EU research project TESTABLE.

- Fix for 1.11.14+
  https://github.com/chamilo/chamilo-lms/commit/c3585401b5215bba48971c7346832d3e55420b28
  (in later commit messages, we also disabled the plugin as we believe no one uses it)

Issue "#91" - 2021-09-11 - Low impact, Medium risk - XSS Vulnerability in HTML5 strings sanitization

A XSS Vulnerability in HTML5 strings sanitization was found in Chamilo in the KSES library. The issue, already known as CVE-2019-20041 and fixed in https://github.com/WordPress/wordpress-develop/commit/b1975463dd995da19bb40d3fa0786498717e3c53

Reported by: Research team in KAIST WSP Lab

- Fix for 1.11.16
  https://github.com/chamilo/chamilo-lms/commit/56df018a8481e65e8c2f0f3f8858a78aca6c3782

Issue "#90" - 2021-09-02 - Low impact, Medium risk - Blind Server-Side Request Forgery (SSRF) in the social network

A Blind Server-Side Request Forgery vulnerability was found in the social network tool, allowing malicious (or fooled) **registered** users of Chamilo to post links to malicious websites that would include attacks in their website information collected through OpenGraph. We do not have a complete solution at this time (we have planned a development for this), and recommend that, if you consider your registered users are not trusted, to disable the social network tool, which can be done from the "Configuration settings" on the administration tab.

Reported by: Dylan Lawhon, Ava Cole, Declan Oberzan, Aidan Quimby @ X-Force Red team, IBM

- Fix for 1.11.16
  Disable the social network tool.
  We also registered a feature request for future versions: https://github.com/chamilo/chamilo-lms/issues/3962

Issue "#89" - 2021-09-02 - Low impact, High risk - XSS in documents

An XSS vulnerability was found in the documents tool, allowing a user to include JS in the link to a document in a learning path. This only requires the capability to trick someone else on clicking a link to a document in Chamilo. We consider XSS as low impact, as they don't affect Chamilo directly but could affect users of Chamilo for other stuff.

Reported by: Dylan Lawhon, Ava Cole, Declan Oberzan, Aidan Quimby @ X-Force Red team, IBM

- Fix for 1.11.16
  https://github.com/chamilo/chamilo-lms/commit/8196eb8e708add895229ac8c3a7688133f23da97

Issue "#88" - 2021-09-02 - Low impact, Medium risk - XSS in learning paths

An XSS vulnerability was found in the learning paths tool, when embedding some content, affecting 1.11.* versions, including 1.11.16.

Reported by: Dylan Lawhon, Ava Cole, Declan Oberzan, Aidan Quimby @ X-Force Red team, IBM

- Fix for 1.11.16
  https://github.com/chamilo/chamilo-lms/commit/ee755bdd3908d9e5689031ccb7fe87e82cd631b5

Issue "#87" - 2021-09-02 - Moderate impact, Low risk - CSRF an XSS in exercises

A CSRF and an XSS vulnerability were found in the exercises tool, results page, affecting 1.11.* versions, including 1.11.16. Due to the fact that it requires access to one particular report, which is only true for specific users, sadly including the platform administrator (except if taken as part of a public course, which requires a voluntary change to the default values of Chamilo), we consider this vulnerability to be low risk as it needs to be targeted to an admin or teacher user to do significant damage **on Chamilo's side**. We categorize CSRF as moderate impact (and XSS as low impact).

Reported by: Dylan Lawhon, Ava Cole, Declan Oberzan, Aidan Quimby @ X-Force Red team, IBM

- Fix for 1.11.16
  https://github.com/chamilo/chamilo-lms/commit/ba8cafc372136b55796098259518acc0205ad34c

Issue "#86" - 2021-08-11 - Moderate impact, Moderate risk - Reflected Cross-site Scripting (XSS)

Multiple instances of Reflected XSS were found throughout the application. This is due an over-reliance of a broken implementation of input sanitization. As a result, an unauthenticated attacker is able to execute arbitrary JavaScript code by deceiving an Admin role user to trigger a specially crafted payload URL, resulting in potential state-changing actions being carried out.

Reported by: Poh Jia Hao, STAR Labs <info@starlabs.sg>

- Fix for 1.11.14
  https://github.com/chamilo/chamilo-lms/commit/03a80ae798644b942ecd15f603eb4b809e10553c

Issue "#85" - 2021-08-11 - High impact, Low risk - Broken Access Control leading to Vertical Privilege Escalation

It was discovered that Session Admin role users are able to modify existing users and escalate their privileges to Platform Admin due to the lack of validation on the user modification form. Since they can create new users as well, Session Admin users are therefore able to escalate their privileges to Platform Admin.
Because session admins are already very high-privileged users, we consider this to be low risk.

Reported by: Poh Jia Hao, STAR Labs <info@starlabs.sg>

- Fix for 1.11.14
  https://github.com/chamilo/chamilo-lms/commit/d2be86122e5bc9f86c7b05a350c49d27989bf099

Issue "#84" - 2021-08-11 - High impact, Moderate risk - Authenticated Blind SQL Injection

Multiple instances of SQL injection were discovered due to the lack of user input sanitization. An authenticated user is able to inject and execute arbitrary SQL queries as a result.

Reported by: Poh Jia Hao, STAR Labs <info@starlabs.sg>

- Fixes for 1.11.14
  https://github.com/chamilo/chamilo-lms/commit/d501af7f9db4d7185f4e44416679f7bda0352c66

Issue "#83" - 2021-08-11 - High impact, Moderate risk - Cross Site Request Forgery (CSRF) leading to Remote Code Execution

It was discovered that the Chamilo administrative panel did not have sufficient anti-CSRF measures, such as the usage of a token. As such, attackers may trick an authenticated Admin user to visit their malicious website and perform a CSRF attack, altering settings on the administrative panel and weakening the security posture of the application. With a set of Trainer role account, the maximum impact for this vulnerability is Remote Code Execution.

Reported by: Poh Jia Hao, STAR Labs <info@starlabs.sg>

- Fixes for 1.11.14
  https://github.com/chamilo/chamilo-lms/commit/e757c63ac8d154ada4bd3c1ebc9628dc1105537f
  https://github.com/chamilo/chamilo-lms/commit/bb3e4b149dbc627e7055f739ceb9bcc86c28c0f3
  https://github.com/chamilo/chamilo-lms/commit/4c36bbc83312bb43197a02d0232d5dbba12ca529

Issue "#82" - 2021-08-11 - High impact, Low risk - Insecure Deserialization and Insecure File Upload leading to Remote Code Execution

It was discovered that an authenticated Trainer role user is able to force the server to send requests to arbitrary domains (SSRF) via a specific end-point. By itself, SSRF allows the attacker to enumerate the internal network by probing private IP addresses for the existence of resources. However, since Trainers can upload files to the server, they are able to upload a [phar](https://www.php.net/manual/en/intro.phar.php) file and then make use of this SSRF vulnerability to invoke the `phar://` protocol to deserialize the uploaded payload and execute system commands.

Reported by: Poh Jia Hao, STAR Labs <info@starlabs.sg>

- Fix for 1.11.14
  https://github.com/chamilo/chamilo-lms/commit/2c8c0ad950c57958fddaccf3116ada9a74c57eff

Issue "#81" - 2021-07-26 - High impact, Low risk - Zero Code RCE in admin

A zero-code Remote Code Injection vulnerability issue was reported with a feature added in 1.11.14, allowing an admin user to upload code in the form of a new plugin. This feature has to be enabled in configuration.php to work, and another user has to trick the admin into uploading the plugin through another vulnerability (making the admin visit its profile). The need to enable plugin upload through configuration.php is why we consider this "low" risk.

Reported almost simultaneously by: Poh Jia Hao, STAR Labs <info@starlabs.sg> and Febin Mon Saji (https://twitter.com/febinrev)

- Fixes for 1.11.14 (which may require fixes for ~~#79~~ to have been applied first)

https://github.com/chamilo/chamilo-lms/commit/0aa0dab9624ed0211edf85f4b50deebc23123421
https://github.com/chamilo/chamilo-lms/commit/46fe4685cc64d12c81ea26b40342e77e53c0e39e

Issue "#80" - 2021-07-26 - Low impact, Low risk - Authenticated XSS

A series of authenticated XSS vulnerabilities were reported in Chamilo forms.

Reported by: Poh Jia Hao, STAR Labs <info@starlabs.sg>

- Fixes for 1.11.x (to be included in 1.11.16)

https://github.com/chamilo/chamilo-lms/commit/e7ebc1db4341eb22b3ccee2ea269baa4202453a1
https://github.com/chamilo/chamilo-lms/commit/0d9add8ec381aa7aedd9c14c9e6cc556093a2e6c
https://github.com/chamilo/chamilo-lms/commit/6c935a64be12c39f25d0009fac482acbe78ab598
https://github.com/chamilo/chamilo-lms/commit/93e89d853ab91548865dd91b41863a77b06d3adc
https://github.com/chamilo/chamilo-lms/commit/78f74d31ea020da718c7ec2fb0da63b1e2c483a0
https://github.com/chamilo/chamilo-lms/commit/ac1b4725c7b4efc457b708a58166eb51c0ab38ea
https://github.com/chamilo/chamilo-lms/commit/55bc1e3bccfbef87dc06e8f9300adf24d3966ba4
https://github.com/chamilo/chamilo-lms/commit/e561531a74b0ea75223bbf5b8eeea0ad7f5cb688
https://github.com/chamilo/chamilo-lms/commit/9815db1ff9aa8f983602d87f820b1970ac0a2a7c
https://github.com/chamilo/chamilo-lms/commit/aa359f9df63fb477fec3f4679de86f667199bf59
https://github.com/chamilo/chamilo-lms/commit/51d2ec0d7697d5052fa1bcb984d01d7bbd15a17a
https://github.com/chamilo/chamilo-lms/commit/58a5c46dc1da4da3210a42ed32890563c07cf64a
https://github.com/chamilo/chamilo-lms/commit/278416857838f80a15c2efb09872fd1529cd6725
https://github.com/chamilo/chamilo-lms/commit/41963f1ddd6012c55b71433444c10346dd9a26a8
https://github.com/chamilo/chamilo-lms/commit/0d8c731a9784ab263aba9ac6bbf056b34c4f3cb2
https://github.com/chamilo/chamilo-lms/commit/93c087fb3f58198f9fa77be9dfb3ed3300439f44
https://github.com/chamilo/chamilo-lms/commit/df68cef1551ee43af5631fc55cc15d55093e1163
https://github.com/chamilo/chamilo-lms/commit/95eef5d3245ec41c2ade4285b4a1b192c29bed9a
https://github.com/chamilo/chamilo-lms/commit/cedce09205408e348811318146c5b9c4c45c9c96

https://github.com/chamilo/chamilo-lms/commit/094fef4af478d71f0b5488b58ceb260376df28f0
https://github.com/chamilo/chamilo-lms/commit/9b16ad40dfb0233f7b461df0b39fc610dba9f26d
https://github.com/chamilo/chamilo-lms/commit/f94d9f6ed709ee93629f1c0654a2a17e2a3042a3
https://github.com/chamilo/chamilo-lms/commit/08b1ae871013660e8f5dd635fc6a064b56286fc3
https://github.com/chamilo/chamilo-lms/commit/83e994cf586366f4bed4cf24a857644e1777a131
https://github.com/chamilo/chamilo-lms/commit/28dc591162272e8ffdcf1afef95b4aa34de6acc3
https://github.com/chamilo/chamilo-lms/commit/ee28c927cf308613781940e3297c51b8eee64096
https://github.com/chamilo/chamilo-lms/commit/122f7bc26793a46d141a9d6919f317f8025f2484
https://github.com/chamilo/chamilo-lms/commit/140f58709926a5c5fea5e49f35be1acba433821d

Issue "#79" - 2021-07-17 - Moderate impact, Low risk - CSRF in global chat and social wall

A CSRF was reported in the users search feature in the social network, allowing an authenticated user to post a message to an admin user, prompting the admin's browser to do a series of unfriendly stuff. This requires the social network or global chat to be enabled and the possibility for the user to write to any other user.

Reported by: Febin Mon Saji (https://twitter.com/febinrev)

- Fix for 1.11.x
  https://github.com/chamilo/chamilo-lms/commit/c75b06adb816565e63f0738c028bd870c49b4de9

Issue "#78" - 2021-07-12 - Low impact, Moderate risk - Reflected XSS in users search in social network

A reflected XSS vulnerability was reported in the users search feature in the social network, allowing for the inclusion of images on remote sites.

Reported by: Pedro Tavares - https://seguranca-informatica.pt

- Fix for 1.11.x
  https://github.com/chamilo/chamilo-lms/commit/3fcc751d5cc7da311532a8756fba5a8778f50ca0

Issue "#77" - 2021-07-12 - Low impact, Moderate risk - Stored XSS in invitation

A stored XSS vulnerability was reported in social network invitation inside Chamilo 1.11.14. Invitations can only be sent by registered users.

Reported by: Pedro Tavares - https://seguranca-informatica.pt

- Fix for 1.11.x
  https://github.com/chamilo/chamilo-lms/commit/de43a77049771cce08ea7234c5c1510b5af65bc8

Issue "#76" - 2021-07-12 - Low impact, Low risk - XSS in install form

An XSS vulnerability was reported in the install procedure of Chamilo 1.11.14. Considering the fact that the install script is only available on non-installed Chamilo portals, and completing the installation requires database credentials to be correct, we consider this a very low risk issue.

Reported by: Pedro Tavares - https://seguranca-informatica.pt

- Fix for 1.11.x
  https://github.com/chamilo/chamilo-lms/commit/dfae49f5dc392c00cd43badcb3043db3a646ff0c

Issue "#75" - 2021-06-18 - Low impact, High risk - Unnecessary information disclosure

The possibility to see and click the breadcrumb navigation element on a page with the error message "Not allowed" was reported as a vulnerability in Chamilo 1.11.x, as it allows the unauthenticated user to obtain additional information about the platform (URL to course home, for example), which is not necessary. The fix to this issue introduces a new configuration.php setting 'hide_breadcrumb_if_not_allowed' which prevents this but has to be manually enabled.

Reported by: Undisclosed

- Fix for 1.11.x
  https://github.com/chamilo/chamilo-lms/commit/9ec3007d29733fca72f97be1d9cbbc4185aa363d

Issue "#74" - 2021-06-11 - Low impact, low risk - Weak protection of password at account creation

The lack of requirement, by Chamilo 1.11.x, for the user to change his/her password at first login was reported as a vulnerability, so we added an administration option (which also requires the creation of an extra field) to force users to change their password the first time they log in.

Reported by: Undisclosed

- Fix for 1.11.x
  https://github.com/chamilo/chamilo-lms/commit/f06ca10afb17c2af718d362861473276078a236a

Issue "#73" - 2021-06-10 - Low impact, low risk - Multiple IP use in single connected user feature

The possibility to use different IP addresses to cheat the "single connected user" feature was reported in Chamilo 1.11.x. It only affects portals that use the prevent_multiple_simultaneous_login configuration option, and it requires the attacker to use different IP addresses (or to spoof them). With the fix, the check is based on the user and is independent of the IP.

Reported by: Undisclosed

- Fix for 1.11.x
  https://github.com/chamilo/chamilo-lms/commit/8e0d4032082d2259ed84f4976ad1c19a40868a24

Issue "#72" - 2021-06-10 - Low impact, low risk - Unprotected access to course files

Unauthorized access to the app/cache/ folder was reported as a security risk, considering it can contain course backups and other exports until the cache is cleared (which is a manual process). Although file names are usually generated with time tokens, links are published to authenticated users, and these could share them with external users, or scripts could reconstruct partial file names and find some of the files. The fix prevents direct access to this folder, which should not cause any issue considering the files are accessed through reader scripts.

Reported by: Undisclosed

- Fix for 1.11.x
  https://github.com/chamilo/chamilo-lms/commit/e70b243b30c1968a9b2d47b158c30937b631e56e

Issue "#71" - 2021-06-08 - Low impact, high risk - Unnecessary availability of web services

The availability of web services was reported as an unnecessary risk for portals with no use of the web services. An option has been added to allow admins to disable the webservices in general (so there is still a need to actively disable them through the configuration.php file).

Reported by: Undiscloed

- Fix for 1.11.x
  https://github.com/chamilo/chamilo-lms/commit/fcb8bfcf8b947eafbadbd0d629951bba87a1e7fa
  https://github.com/chamilo/chamilo-lms/commit/98d2668e271f554d3bd9e8e433176da3b3eb675a

Issue "#70" - 2021-06-04 - Low impact, high risk - XSS in web service script

An XSS vulnerability was reported on a script used for practical purposes in the configuration of web services. This does not affect the security of webservices, but could be used to lure users into navigating to this script.

Reported by: Undisclosed

- Fix for 1.11.x
  https://github.com/chamilo/chamilo-lms/commit/b9bb577010a0e111e1a9e6ef37a2001619b131a8

Issue "#69" - 2021-05-25 - Moderate impact, moderate risk - Server info disclosure

A server info disclosure vulnerability has been discovered in 1.11, allowing non authenticated users to take some actions (part of the Chamilo installation procedure) that could reveal server information.

Reported by: Undisclosed

- Fix for 1.11.x
  https://github.com/chamilo/chamilo-lms/commit/6946b7c93e17d59cecf7b5cd7b5ba67aeaa7874a

Issue "#68" - 2021-05-21 - Low impact, low risk - XSS in forum

An XSS vulnerability was reported in Chamilo 1.11 in the forum, allowing authenticated users to include a XSS attack in their posts.

Reported by: Undisclosed

- Fix for 1.11.x
  https://github.com/chamilo/chamilo-lms/commit/63bf4ad8481e9d53c10bb1ed5f5e45837a98145b

Issue "#67" - 2021-05-27 - High impact, very high risk - Unauthenticated SQL injection - CVE-2021-34187

An unauthenticated SQL injection was reported in Chamilo 1.11 and (dev version of) 2.0. Considering 2.0 is not used in production yet, we have fixed it but the fixes below do not mention it.

Reported by Kutlymurat Mambetniyazov (@manfromkz from NitroTeam.kz).

- Fix for 1.11.x
  https://github.com/chamilo/chamilo-lms/commit/f7f93579ed64765c2667910b9c24d031b0a00571 (this creates an issue with sessions search, corrected by the following)
  https://github.com/chamilo/chamilo-lms/commit/26e9b8f90838913564fa65db67dfa94b576ec54c

Issue "#66" - 2021-05-21 - High impact, very low risk - Authenticated RCE in accessory script

An authenticated RCE (uploading htaccess files) was reported in Chamilo 1.11.x

Reported by Andrej Spuler (@netw0r)

- Fix for 1.11.x
  https://github.com/chamilo/chamilo-lms/commit/2e5c004b57d551678a1815500ef91524ba7bb757
  https://github.com/chamilo/chamilo-lms/commit/8ba572397445477d67ca55453fd8f29885bb19e5
  https://github.com/chamilo/chamilo-lms/commit/905a21037ebc9bc5369f0fb380177cb56f496f5c

Issue "#65" - 2021-05-15 - High impact, very high risk - Unauthenticated SQL injection in plugin

An unauthenticated SQL injection was reported in a Chamilo 1.11.x plugin.

Reported by Andrej Spuler (@netw0r)

- Fix for 1.11.x
  https://github.com/chamilo/chamilo-lms/commit/6a98e32bb04aa66cbd0d29ad74d7d20cc7e7e9c5

Issue "#64" - 2021-05-14 - Low impact, low risk - XSS in course document title on upload

An XSS vulnerability requiring at least student access and course groups access, or teacher access was reported on the course title in Chamilo 1.11.x.

Reported by Andrej Spuler (@netw0r)

- Fix for 1.11.x
  https://github.com/chamilo/chamilo-lms/commit/cf84be1ca1d9a08ad1341dfbf8df475b13a89072

Issue "#63" - 2021-05-14 - Low impact, moderate risk - XSS in course documents

An XSS vulnerability requiring at least student access and course groups access, or teacher access was reported in the documents editor in Chamilo 1.11.x, but there are configuration options to avoid it.

Reported by Andrej Spuler (@netw0r)

This will be attended in version 2.0 of Chamilo.

Issue "#62" - 2021-05-14 - Low impact, low risk - XSS in course description

An XSS vulnerability requiring teacher access was reported on the course description in Chamilo 1.11.x.

Reported by Andrej Spuler (@netw0r)

- Fix for 1.11.x
  https://github.com/chamilo/chamilo-lms/commit/19189a91d1eac9aa204b9439b82e3e73c8ac2e03

Issue "#61" - 2021-05-14 - Low impact, very low risk - XSS in course name

An XSS vulnerability requiring admin access was reported on the course name in Chamilo 1.11.x.

Reported by Andrej Spuler (@netw0r)

- Fix for 1.11.x
  https://github.com/chamilo/chamilo-lms/commit/fd54f6194285f949c86060d3b2a7967b43689480

Issue "#60" - 2021-05-13 - High impact, very low risk - SQL injection vulnerability in sessions (requires admin perms)

An authenticated SQL injection requiring admin permissions was reported on Chamilo 1.11.x.

Reported by Andrej Spuler (@netw0r)

- Fix for 1.11.x
  https://github.com/chamilo/chamilo-lms/commit/93ed46451927dd7d5826cde9e08a2b438b9220e0

Issue "#59" - 2021-05-13 - High impact, low risk - Unauthenticated SQL injection vulnerability when a module is enabled

An unauthenticated SQL injection only exploitable when a specific module is enabled was reported in Chamilo 1.11.14.

Reported by Andrej Spuler (@netw0r)

- Fix for 1.11.14
  https://github.com/chamilo/chamilo-lms/commit/36149c1ff99973840a809bb865f23e1b23d6df00
  https://github.com/chamilo/chamilo-lms/commit/f398b5b45c019f873a54fe25c815dbaaf963728b

Issue "#58' - 2021-05-12 - High impact, very low risk - LFI/RCE vulnerability in users import

An authenticated LFI (leading to remote code execution if a specific wrapper is available on the Chamilo server) has been reported on chamilo 1.11.x.

Reported by Andrej Spuler (@netw0r)
CVE-2021-32925

- Fix for 1.11.x
  https://github.com/chamilo/chamilo-lms/commit/e71437c8de809044ba3ae1b181d70857c050a3e9

Issue "#57" - 2021-04-20 - High impact, very low risk - Command Injection vulnerability in course_intro_pdf_import.php

A vulnerable section of code has been commented out in previous versions, but its presence is easily flagged as a vulnerability.

Reported by {undisclosed}.

- Fix for 1.11.x
  https://github.com/chamilo/chamilo-lms/commit/120f37ccfb61eec87550357179964672fe0a4dea

Issue "#56" - 2021-04-20 - Low impact, high risk - Scripts accessible without authentication

Some scripts were accessible without authentication, that could lead to some data leakage in specific circumstances.

Reported by {undisclosed}.

- Fix for 1.11.x
  https://github.com/chamilo/chamilo-lms/commit/e32020722cbafe08a96bb26a8972c32371334bc6
  https://github.com/chamilo/chamilo-lms/commit/64cc7e8bd3ab3cd7d9c840036166a8834dc2184d

Issue "#55" - 2021-04-20 - Moderate impact, high risk - Unauthenticated SSRF and open redirect in proxy.php

Server side request forgery and open redirect in proxy.php, a minor script used in some specific cases for portals behind a proxy. We have disabled this script by default now.

Reported by {undisclosed}.

- Fix for 1.11.x
  https://github.com/chamilo/chamilo-lms/commit/e32020722cbafe08a96bb26a8972c32371334bc6

Issue "#54" - 2021-04-20 - Moderate impact, low risk - Reflected XSS in access_url.php

Reflected XSS vulnerability in access_url.php, a minor script to get the list of URLs (through SOAP) on a multiple URLs setup.

Reported by {undisclosed}.

- Fix for 1.11.x
  https://github.com/chamilo/chamilo-lms/commit/640a40ea7838545e49e7215791737cf4b50ae0b8
  https://github.com/chamilo/chamilo-lms/commit/025577a541c9ed92dbd5bb24f14b3c3b26c0c9b3

Issue "#53" - 2021-04-20 - Moderate impact, moderate risk - Reflected XSS in template.lib.php

Reflected XSS vulnerability in template.lib.php.

Reported by {undisclosed}.

- Fix for 1.11.x
  https://github.com/chamilo/chamilo-lms/commit/a669ca3204f54f1fa9d105ac4ad8e593fb951951

Issue "#52" - 2021-04-20 - Moderate impact, low risk - Authenticated reflected XSS

It is possible to trigger an XSS vulnerability in documents through a specially crafted URL. However, it requires the user to be authenticated (except in the case of open courses).

Reported by {undisclosed}.

- Fix for 1.11.x
  https://github.com/chamilo/chamilo-lms/commit/c04a9199fb7c25d266bb7fae578c61ee3f838a76

Issue "#51" - 2021-04-20 - High impact, high risk - Multiple unauthenticated SQL injections

SQL injections possible through AJAX calls.

Reported by {undisclosed}.

- Fix for 1.11.x
  https://github.com/chamilo/chamilo-lms/commit/473035f3a2e01b3b8a5e8c6a47bb62320fb750a5
  https://github.com/chamilo/chamilo-lms/commit/58bbe957a416e56dd9e8d0c39fd7199a8f9aa615
  https://github.com/chamilo/chamilo-lms/commit/9fb379cab5cf8235e08719fa825cab6c3cc0f068

Issue "#50" - 2021-04-20 - High impact, moderate risk - Webservices authenticated arbitrary file upload

Security key improperly checked in API calls.

Reported by {undisclosed}.

- Fix for 1.11.x
  https://github.com/chamilo/chamilo-lms/commit/dd33807b3d0cc237cdc08aa4c219d71cb2972533

Issue "#49" - 2021-04-20 - High impact, high risk - API authentication bypass

Security key improperly checked in API calls.

Reported by {undisclosed}.

- Fix for 1.11.x
  https://github.com/chamilo/chamilo-lms/commit/d467daefd4dcd05bbe3b3050938ee2c8fe1a0aa8
  https://github.com/chamilo/chamilo-lms/commit/a4ffdc315dfe4a059cfb0cd8e9c49780dd0c1a0f

Issue "#48" - 2021-04-17 - Critical impact, high risk - Remote Code Execution

Attacker may execute code remotely in a specific directory if able to upload a file there and the installation documentation for Chamilo suggests enabling file upload there, so it is the case by default.

Rating: https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:F/RC:C

Reported by M. Cory Billington (@_th3y).
CVE: http://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-31933

- Fix for 1.11.x
  https://github.com/chamilo/chamilo-lms/commit/f65d065061a77bb2e84f73217079ce3998cf3453
  https://github.com/chamilo/chamilo-lms/commit/229302139e8d23bf6862183cf219b967f6e2fbc1

Issue "#47" - 2021-01-28 - Critical impact, high risk - SQL injection

An unauthenticated SQL injection vulnerability has been detected in Chamilo 1.11.14. Unauthenticated SQL injections are considered critical because they allow... well, unauthenticated users to affect the database. This type of vulnerability is historically extremely rare in Chamilo. We highly recommend applying the following patch **as soon as possible** to your Chamilo installation.

Reported by {undisclosed}.

- Fix for 1.11.x
  https://github.com/chamilo/chamilo-lms/commit/e8332fd9d5607ae7866e27936b4376ea1053ae03

Issue "#46" - 2021-01-28 - High impact, moderate risk - Path traversal

Authenticated path traversal. Requires authentication but can read files on the server.

Reported by {undisclosed}.

- Fix for 1.11.x
  https://github.com/chamilo/chamilo-lms/commit/eb823e7ff52cf9062205a58ffd9d9991975be6d8
  https://github.com/chamilo/chamilo-lms/commit/5f39ba7c8dae8cb19e4e86718f09c396a4f26bec (this one fixes an issue introduced by the previous commit)

Issue "#45" - 2021-01-21 - Moderate impact, moderate risk - XSS vulnerability in agenda

An authenticated user with the right to edit calendar items can introduce an XSS attack into the agenda page.

Reported by Ali Oğuz from https://www.netsparker.com/.
CVE: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26746

- Fix for 1.11.x
  https://github.com/chamilo/chamilo-lms/commit/d939402d83bf68af5377b629883d8e5437d843ec

Issue "#44" - 2021-01-14 - Moderate impact, moderate risk - Cross Site Request Forgery in calendar

Chamilo LMS version 1.11.14 and prior contain a CSRF vulnerability that allows a user with permissions to edit calendar event (including personal agenda) to inject JS code that enable the CSRF vector to be exploited.
This requires privileged access, but could be abused by low-access level users if the proper conditions are met.

Thanks to Maheshkumar Darji for reporting the issue to us.

- Fix for 1.11.x
  https://github.com/chamilo/chamilo-lms/commit/e4781a7d15aa4df1564be4bae5d5db554d2941c8

Issue "#43" - 2020-05-04 - Moderate impact, moderate risk - XSS in personal profile and messages

Chamilo LMS version 1.11.10 contains several additional XSS vulnerabilities in the personal profile edition form and the personal messaging, affecting the user him/herself and social network friends.

Thanks to Emil Virkki for reporting the issue to us.

- Fix for 1.11.x
  https://github.com/chamilo/chamilo-lms/commit/ce56951fc3c22178b1bb0b499fe8a3c108f8502d
  https://github.com/chamilo/chamilo-lms/commit/c32499e239531f7e99f872d68827b6f7cc66146c

Issue "#42" - 2020-04-23 - High risk, low impact - XSS in extended user's profile fields

Chamilo LMS version 1.11.10 contains an XSS vulnerability in the personal profile edition form, affecting the user him/herself and social network friends.

Thanks to Vu Van Tien for reporting the issue to us.

- Fix for 1.11.x
  https://github.com/chamilo/chamilo-lms/commit/aced30eaed1cb491c44aec1c37d5b3fc1c28f434

Issue "#41" - 2020-04-22 - Medium risk, high impact - CSRF and privilege escalation via CSRF

Chamilo LMS version 1.11.10 contains a CSRF vulnerability and a privilege escalation vulnerability in the (administrative) user edition form. This requires specifically targeting an admin user

Thanks to Toản Đăng for reporting the issue to us.

- Fix for 1.11.x
  https://github.com/chamilo/chamilo-lms/commit/bf50545e848805c9f123e6736eeba2edd7327bbc

Issue "#40" - 2019-04-14 - Low risk, moderate impact - XSS

Chamilo LMS version 1.11.8 contains an XSS vulnerability in the course forum titles.

Thanks to HexPandaa for reporting the issue to us.

- Fixes for 1.11.x
  https://github.com/chamilo/chamilo-lms/commit/ee878212d691d2f3c6bab92002afb599846d3e0f

Issue "#39" - 2019-02-25 - High risk, high impact - RCE, File upload

Chamilo LMS version 1.11.8 contains a remote code execution and a file upload vulnerability, already moderated by the fix in issue 36, but still available to privileged users. You will need to run composer update once the patch is applied, as we use an additional external library to remove the flaw (PHP 5 does not allow for filtering of classes before unserialize).

Thanks to 0xecute for reporting the issue to us.

- Fixes for 1.11.x (through a set of commits)
  https://github.com/chamilo/chamilo-lms/pull/2821/files

Issue "#38" - 2018-12-17 - Low risk, high impact - XXE

This is a special case because the issue was reported on the 2018-12-17 but took an unusually long time to fix because it affected one of the libraries we use the most for XML parsing, with no other solution than to switch from one library to another for standard import formats.

We thank Pierre Pailleux for reporting the issue to us.

- Fixes for 1.11.x
  https://github.com/chamilo/chamilo-lms/pull/2778 (this page contains a list of fixes that all need to be applied)

Issue "#37" - 2018-12-18 - Low risk, moderate impact - XSS

This is a special case because the issue was reported on the 2018-12-18 and fixed almost immediately, but we forgot to report it.
Chamilo LMS version 1.11.8 contains an XSS vulnerability in the tickets module.

We thank Pierre Pailleux for reporting the issue to us.

- Fixes for 1.11.x
  https://github.com/chamilo/chamilo-lms/tree/54d05c11b97b20e5286b9cb5ce9e9670a96d3c64
  https://github.com/chamilo/chamilo-lms/tree/bec1fd1681fc1edf21e697a3b561897f7a3ea9f5

Issue "#36" - 2019-02-25 - Moderate risk, high impact - Privilege escalation/RCE

Chamilo LMS version 1.11.8 contains a privilege escalation risk enabled by the existence of a flaw in the deprecated code of the text-to-speech module Nanogong. This one is tricky to apply through a Chamilo update because it requires the main/inc/lib/nanogong directory to be removed. If you are in developer mode, a simple "composer update" will remove the directory once you updated Chamilo to 1.11.10 or later.

Thanks to 0xecute for reporting the issue to us.

- Fixes for 1.11.x
  https://github.com/chamilo/chamilo-lms/commit/2164d36f0b0f61f342dff08d7ef977634e05e876

Issue '#35" - 2019-01-23 - High risk, moderate impact - Unauthenticated personal data leak

Chamilo LMS version 1.11.8 contains the following flaws (additional to the previously reported flaws):

- 2 leaks of user firstname, lastname, picture and e-mail through an AJAX call, not requiring authentication

Thanks to 0xecute for reporting the issue to us.

- Fixes for 1.11.x
  https://github.com/chamilo/chamilo-lms/commit/481267293eba109ae329ff201565577fcf5b2202
  https://github.com/chamilo/chamilo-lms/commit/2937cf24cf6842c2f6ce9422028a1e5f9842ef09
  https://github.com/chamilo/chamilo-lms/commit/e46377515fb33eb573c4bfcbcee173aac60c1393
  https://github.com/chamilo/chamilo-lms/commit/40560f93229595bd1465c71e57abe0563b166597
  https://github.com/chamilo/chamilo-lms/commit/1c82459f142e67636b9241cef1d46b2b927547dd
  https://github.com/chamilo/chamilo-lms/commit/c245b03308f8274b93f2a39e5435d5e9e4b6aecf

These security patches will be part of version 1.11.10 and versions 2.0 and up.

Issue '#34" - 2019-01-14 - Moderate risk, moderate impact - XSS and unauthorized access

Chamilo LMS version 1.11.8 contains a few XSS vulnerabilities in the social messaging, and an XSS and an unauthorized access in the tickets reporting system. All require authenticated access, so we do not consider them a high risk or impact.

Thanks to João Arnaut, Dognaedis for reporting the issue to us.

- Fix for 1.11.x
  https://github.com/chamilo/chamilo-lms/commit/33e2692a37b5b6340cf5bec1a84e541460983c03

These security patches will be part of version 1.11.10 and versions 2.0 and up.

Issue '#33" - 2018-12-13 - Moderate risk, high impact - SQL Injection

Chamilo LMS version 1.11.8 contains an SQL injection, allowing users with access to the sessions catalogue (which may optionally be made public) to extract and/or modify database information. We recommend any administrator using sessions and having enabled the sessions catalogue to apply the patch ASAP.

We thank Pierre Pailleux for reporting the issue to us.

- Fix for 1.11.x
  https://github.com/chamilo/chamilo-lms/commit/bfa1eccfabb457b800618d9d115f12dc614a55df

These security patches will be part of version 1.11.10 and versions 2.0 and up.

Issue '#32" - 2018-11-28 - Low risk - More XSS and path disclosure issues

Chamilo LMS version 1.11.8 contains two XSS vulnerabilities, one in the gradebook dependencies tool and one in the social groups tool, allowing authenticated users to affect other users, under specific conditions of permissions granted by administrators. This is considered "low risk" due to the nature of the feature it exploits. Also, some paths disclosure appeared in the case of a platform configured as "test" platform and showing PHP notice and warning messages on screen (which is not recommended).

We thank Pierre Pailleux for reporting the issues to us.

- Fix for 1.11.x
  - https://github.com/chamilo/chamilo-lms/commit/5e61c2b0fcc938ca687b8d4e593b1500aa52a034
  - https://github.com/chamilo/chamilo-lms/commit/da8a93eea4b438e9d0433b7cb989d3ecafbaf65e
  - https://github.com/chamilo/chamilo-lms/commit/15e49c1737b27f78aca7f948c6634c68753e51cf
  - https://github.com/chamilo/chamilo-lms/commit/814049e5bd5317d761dda0ebbbc519cb2a64ab6c

These security patches will be part of version 1.11.10 and versions 2.0 and up.

Issue '#31' - 2018-11-18 - Moderate risk - SQLi, Reflected and Stored XSS vulnerabilities

Chamilo LMS version 1.11.8 contains several vulnerabilities of different levels of risk and criticality.

Two SQL injection issues require admin access, so although very high-damage vulnerabilities, we lowered the risk because they require very specific access to administration pages.
Several reflexted XSS vulnerabilities have been reported in a mix of admin and public pages, so we raised the risk to moderate.
One stored XSS vulnerability was found on a course description page that requires user access to the specific course (low risk).

We thank Zekvan Arslan and the Netsparker Web Application Security Scanner team for their work finding and reporting these issues. A first advisory was sent to the wrong e-mail in July but we only caught it in November. A special thank to the Netsparker team for finding the right channels and being persistent on that one. We couldn't have made this safe report without you.

- Fix for 1.11.x
  - https://github.com/chamilo/chamilo-lms/commit/d13365c19486d0783426a8c5315310a406d5be01

This security patch will be part of version 1.11.10 and versions 2.0 and up.

Issue '#30" - 2018-11-13 - Low risk - More XSS in agenda

Chamilo LMS version 1.11.8 contains an additional series of XSS vulnerabilities in the agenda tool, allowing authenticated users to affect other users (sharing the same agenda events). This is considered "low risk" because, due to the nature of the feature it exploits, it is either necessary to be a teacher in a course or to be a student that was explicitly allowed by a teacher to edit agenda events. As such, the existence of the issue would only (in theory) affect open platforms or platforms with malicious (and security-skilled) teachers.

We thank Pierre Pailleux for reporting the issues to us.

- Fix for 1.11.x
  - https://github.com/chamilo/chamilo-lms/commit/099ec4117ed4aa6bd966f1928718fe69a0773723
  - https://github.com/chamilo/chamilo-lms/commit/d9c37bf1f3e43b67b4f5b54938af2c45a51db309

These security patches will be part of version 1.11.10 and versions 2.0 and up.

Issue '#29' - 2018-10-06 - Moderate risk - XSS on registration page

Chamilo LMS version 1.11.8 contains an XSS vulnerability in the user registration form.
This represents a "moderate" risk because it is only available to open portals (Chamilo portals that allow registration by anyone). However, on these portals, it might have serious implications for administrators checking the users list on the administration page. As such, we urge all admins or open portals to update their Chamilo 1.11.8 portals with the patch provided below (a one-liner easily applied by hand).

See https://packetstormsecurity.com/files/149711/chamilolms1118fn-xss.txt

While we thank the author ("Cakes") for reporting this issue, we disapprove of the immediate publication. Our politic is to provide a patch under 72h of being notified, as far as humanly possible. We received no notification before this went public. Contact details are available in the first section of this page.
Also, while reporting it in "white hat" mode, "Cakes" also tested it on a live public portal, which is not really what we would expect where the report indicates it was tested on a different IP address.
Despite these 2 latest detected vulnerabilities, we believe (based on security reports of competitors) Chamilo remains the safest LMS around.

Initially published by "Cakes".

- Fix for 1.11.x
  - https://github.com/chamilo/chamilo-lms/commit/a248539a5d9af7d4c261faa5adfc7f0394e9fd48

This security patch will be part of version 1.11.10 and versions 2.0 and up.

Issue '#28' - 2018-10-05 - Low risk - XSS in agenda

Chamilo LMS version 1.11.8 contains an XSS vulnerability in the agenda tool, allowing authenticated users to affect other users (sharing the same agenda events). This is considered "low risk" because, due to the nature of the feature it exploits, it is either necessary to be a teacher in a course or to be a student that was explicitly allowed by a teacher to edit agenda events. As such, the existence of the issue would only (in theory) affect open platforms or platforms with malicious (and security-skilled) teachers.

See details here: https://packetstormsecurity.com/files/149679/chamilolms1118-xss.txt

While we thank the author ("Cakes") for reporting this issue, we disapprove of the immediate publication. Our politic is to provide a patch under 72h of being notified, as far as humanly possible. We received no notification before this went public. Contact details are available in the first section of this page.

Initially reported by "Cakes".

- Fix for 1.11.x
  - https://github.com/chamilo/chamilo-lms/commit/39b3162698455246dbfe791b2f9415c629f52120

This security patch will be part of version 1.11.10 and versions 2.0 and up.

Issue '#27' - 2018-08-06 - Moderate risk - Unauthenticated remote code execution

Chamilo LMS version 1.11.x contains an unserialization vulnerability in a POST parameter that can result in Unauthenticated remote code execution. This attack is only exploitable by users with access to the course maintenance tool (teachers and admins), reason for which we reduced the risk to Moderate.

This affects versions 1.11 of Chamilo only.

Initially reported by e-mail by a contact self-called "shuimugan".

- Fix for 1.11.x
  - https://github.com/chamilo/chamilo-lms/commit/ecb18907a7fec22402411aa873382a4bd06cb07d

This security patches will be made available as part of Chamilo 1.11.8 and superior.

Issue '#26' - 2018-07-23 - Critical risk - Unauthenticated remote code execution

Chamilo LMS version 11.x contains an Unserialization vulnerability in the "hash" GET parameter for the api endpoint located at /webservices/api/v2.php that can result in Unauthenticated remote code execution. This attack appear to be exploitable via a simple GET request to the api endpoint. This vulnerability appears to have been fixed in After commit 0de84700648f098c1fbf6b807dee28ec640efe62. CVE-2018-1999019 has been assigned to this issue.

This affects versions 1.11 of Chamilo only.

Initially reported by Indiana Moreau on https://github.com/chamilo/chamilo-lms/issues/2532

- For 1.11.x
  - https://github.com/chamilo/chamilo-lms/commit/0de84700648f098c1fbf6b807dee28ec640efe62

This security patches will be made available as part of Chamilo 1.11.8 and superior.

Issue '#25' - 2018-05-31 - Moderate risk - Data leak

A flaw in the logic of the "Who is online" page made it possible for unauthenticated users to get a list of names and pictures of the users currently online on the Chamilo portal. We consider it a moderate risk as it is available to the public but only through using specific URLs not directly visible to the public, and because it only makes names and pictures available (no other private information) and only for users connected now or in the past few minutes.

This affects versions 1.11 of Chamilo and possibly previous versions.

This was kindly mentioned by Jurjen de Jonge of HVA.nl on 23/5/2018 but only received by us (due to e-mail issues on our side) on the 31/5/2018. A fix was provided a few hours after finally receiving the report. The fix removes the information if the option "see connected users from the portal homepage" has been disabled. By default, this option is enabled in Chamilo, so for security reasons, we recommend admins to disable it when installing their portal.

- For 1.11.x
  - https://github.com/chamilo/chamilo-lms/commit/d400657bfa7ca08ca7a26abb73f607244cc48e73

No fix was provided for 1.10.x at this point as we consider this security issue a moderate risk.

This security patches will be made available as part of Chamilo 1.11.8 and superior.

Issue '#24' - 2018-04-09 - Low risk - Data leak

A flaw in the logic of the assignments tool in Chamilo made it possible for **registered users** to access the assignments provided by all other users in the same course.

This affects versions 1.11 of Chamilo (and probably previous versions), **but** you need a user account, to have access to a course and that the assignments tool be enabled in order to abuse this flaw. If all these conditions are combined, you could effectively download assignments from all other students even if you configured that assignments are not shared.

This was kindly reported by Jan Derriks of HVA.nl on the 9/4/2018. A fix for 1.11 was provided 40 minutes later.

- For 1.11.x
  - https://github.com/chamilo/chamilo-lms/commit/00f3e4a6506035674a58ccdf4ebe098bd6f607e3

No fix was provided for 1.10.x at this point as we consider this security issue a low risk.

These security patches will be made available as part of Chamilo 1.11.8 and superior.

Issue '#23' - 2017-02-09 - Moderate risk - PHP File Upload

A flaw in the elfinder extension to CKeditor in Chamilo was reported to us by Sandro "guly" Zaccarini.

This affects versions 1.10 and 1.11 of Chamilo, **but** you need a user account, that the social network be enabled **and** a special script to hack the upload method. This is why, although a PHP file upload issue would usually be marked as "High" or "Very high" risk, this has been lowered to "Moderate" risk.

We have made patches available to development versions of both 1.10 and 1.11:

- For 1.10.x
  - https://github.com/chamilo/chamilo-lms/commit/501d19fed7773c7f5749cfa8d97cc8c7441fc7b1
- For 1.11.x
  - https://github.com/chamilo/chamilo-lms/commit/337c3e6d254a2eae161f6e1405b8ab2fc01ef35f
  - https://github.com/chamilo/chamilo-lms/commit/ac8a66b240bcf92a9e83ec2f4c7e829747269a00

These security patches will be made available as part of Chamilo 1.11.4.

Issue '#22' - 2016-12-26 - Moderate risk - PHPMailer shell escaping flaw

A flaw in the PHPMailer library, used in Chamilo LMS <=1.* was reported to us by Peter Bex of more-magic.net, and initially identified by Hanno Böck.

Fixes for different versions of Chamilo are provided below, matching our max 72h response time policy:

- For 1.9.x
  - https://github.com/chamilo/chamilo-lms/commit/816a809da5446866fbb4b2101898027ec328e9b9
- For 1.10.x
  - https://github.com/chamilo/chamilo-lms/commit/ea335267dd96e6a3ea2bec53022c86115f55fe32
- For 1.11.x
  - https://github.com/chamilo/chamilo-lms/commit/069845f08759cce4aa3693235e8d0a9a131ca35b

Issue '#21' - 2016-07-15 - Moderate risk - User Input Sanitation

A series of user input data were reported as unsanitized in 1.10.6. This was reported by Echelon team (npo-echelon.ru) and automatically detected by static code analyzer AppChecker. As far as we could check, these require course access and, as such, will not affect non-public courses. You either have to have an open-access platform or an open course inside your platform to be affected.

Fixes for these vulnerabilities can be found here: https://github.com/chamilo/chamilo-lms/commit/52ef413e2719be2da521beb83a476d91468ef5e7
We have added additional filtering as well, available here: https://github.com/chamilo/chamilo-lms/commit/2a47c02329fb8dee04a6b6425c9ee7601c6f32e2

These fixes have been included in Chamilo 1.10.8 and all future versions.

Issue '#20' - 2016-02-15 - Moderate risk - (messageId)

A rogue (not reported through official canals and include a public exploit) security issue was reported on 17/02/2016 by Lawrence Amer about being able to hijack another person's session through the handling of a crafted work in the assignments tool. This requires low-permissions access (student in a course) but could allow a student to hijack a teacher or admin's session.

Fixes for different versions of Chamilo are provided below, matching our max 72h response time policy:

- For 1.9.x
  - https://github.com/chamilo/chamilo-lms/commit/d24f81b60e0a788a1dea4272ebe4a342f8874623
- For 1.10.x
  - https://github.com/chamilo/chamilo-lms/commit/c3b9a10e7c9ad04e1cc3437848a99867cb5067ad

Issue '#19' - 2016-02-15 - Moderate risk - (messageId) Delete Post Vulnerability

A rogue (not reported through official canals and include a public procedure on how to exploit) security issue was reported on 15/02/2016 by Lawrence Amer about accessing other people's messages in the Chamilo social network, and giving the ability to delete the others' messages. Given the fact that messages are also sent by e-mail, we do not consider the deletion of other people's messages a high risk. However, accessing the messages themselves can be considered a high private information access vulnerability.

Fixes for different versions of Chamilo are provided below, matching our max 72h response time policy:

- For 1.9.x
  - https://github.com/chamilo/chamilo-lms/commit/9b9de176d3651f5a9a59fd3ae0bf63a098392027
- For 1.10.x
  - https://github.com/chamilo/chamilo-lms/commit/e45079df7a1bf31bbcdd9b1d22d8c23cf76fd1db

Issue '#18' - 2015-05-02 - Low-Moderate risk - URL hijacking/spoofing

A URL spoofing vulnerability has been reported by Luis Eduardo Jácome V. in Chamilo LMS 1.9.10.2 and all previous versions, allowing malintentionned crackers to modify an URL like:

- http://chamilo.org/main/link/link_goto.php?[...]&link_url=[original-redirect-url]

to

- http://chamilo.org/main/link/link_goto.php?[...]&link_url=[malign-redirect-url]

Because the change is clearly visible in the URL, we don't consider this vulnerability to represent a high risk to the user, but we still consider this a valid vulnerability, which is why we have provided the following fix, that you can freely apply to your 1.9.* installation. These changes will effectively ignore the link_url parameter and only take into account the link_id which is stored in the database, making it impossible to hack through the same channel. Very complicated circumstances prevented us from publishing the fix on this page in a timely manner, but the commits were sent several days ago already.

https://github.com/chamilo/chamilo-lms/commit/aa052c08b9f4bbde686572c66dc0301ac7a480b8
https://github.com/chamilo/chamilo-lms/commit/23f2e7520be2c0c9e77e58d508023f39afb82f6c
https://github.com/chamilo/chamilo-lms/commit/aeac10a06115a810bd630f04d55f452c51be35d5
https://github.com/chamilo/chamilo-lms/commit/84bba539d632957447832a01cf2e2c4035ed6dbf

Or, in more details:

```
diff --git a/main/inc/lib/link.lib.php b/main/inc/lib/link.lib.php
index 875f048..eb3b156 100755
--- a/main/inc/lib/link.lib.php
+++ b/main/inc/lib/link.lib.php
@@ -103,6 +103,28 @@ class Link extends Model

         return false;
     }
+
+    /**
+    *
+    * Get link info
+    * @param int link id
+    * @return array link info
+    *
+    **/
+    public static function get_link_info($id)
+    {
+        $tbl_link = Database:: get_course_table(TABLE_LINK);
+        $course_id = api_get_course_int_id();
+        $sql = "SELECT * FROM " . $tbl_link . "
+                WHERE c_id = $course_id AND id='" . intval($id) . "' ";
+        $result = Database::query($sql);
+        $data = array();
+        if (Database::num_rows($result)) {
+            $data = Database::fetch_array($result);
+        }
+
+        return $data;
+    }
 }

 /**
diff --git a/main/link/link_goto.php b/main/link/link_goto.php
index 75163bb..101967f 100755
--- a/main/link/link_goto.php
+++ b/main/link/link_goto.php
@@ -21,16 +21,20 @@
 require_once '../inc/global.inc.php';
 $this_section = SECTION_COURSES;

-$link_url = html_entity_decode(Security::remove_XSS($_GET['link_url']));
-$link_id = intval($_GET['link_id']);
+require_once api_get_path(LIBRARY_PATH).'link.lib.php';

+$this_section = SECTION_COURSES;
+
+$linkId = intval($_GET['link_id']);
+
+$linkInfo = Link::get_link_info($linkId);
+$linkUrl = html_entity_decode(Security::remove_XSS($linkInfo['url']));
 // Launch event
-event_link($link_id);
+event_link($linkId);

 header("Cache-Control: no-store, no-cache, must-revalidate");   // HTTP/1.1
 header("Cache-Control: post-check=0, pre-check=0", false);
 header("Pragma: no-cache");                                     // HTTP/1.0
-header("Location: $link_url");
-
-// To be sure that the script stops running after the redirection
+header("Location: $linkUrl");
 exit;
```

The fix has already been applied in prevision of version 1.10.0 and future versions.

Issue '#17' - 2015-03-19 - Moderate risk - XSS & CSRF vulnerabilities

A series of XSS and CSRF vulnerabilities were reported on the 2/3/2015 by Rehan Ahmed. After careful consideration and a fruitful exchange, we released different patches (find them individually in the Chamilo changelog for 1.9.10.2) that cover these vulnerabilities.

In the official report, the author mentions the patch release to be 1.9.11. However, our bugfix releases policy enforces the use of the 1.9.10.2 number for this release. As of this writing, 1.9.11 does not (and will not) exist, it is a misnaming of 1.9.10.2.

This is considered a moderate risk because most of these require to be an authenticated user in order to exploit them. On privately-managed portals, this is usually not an issue, but on open campuses, it is.

Initial report: received by e-mail on 2/3/2015
Proper report: #7564
Fix: The fix is to upgrade to Chamilo LMS 1.9.10.2, released today. The changelog contains the individual commits required to fix the vulnerabilities manually.
Affected versions: These vulnerabilities are likely to affect all previous versions of Chamilo LMS

If you are using **any** 1.9.x version of Chamilo, 1.9.10.2 is a minor version, so upgrading is **only** a matter of overwriting the current Chamilo code (removing the home/ directory in the **new** version package is recommended before you overwrite, in case you have a customized homepage).

If you require assistance applying those fixes, Chamilo Official Providers are trained to help you out in a professional manner.

Issue '#16' - 2015-01-25 - High risk - SQL injection vulnerability in several queries

A series of security issues have been reported on the 9/12/2014 by Kacper Szurek. Because these vulnerabilities potentially affected numerous parts of the code, we took some time to finish a complete review of Chamilo and decided to publish the fix as part of Chamilo LMS 1.9.10.

This is considered high-risk because we could not measure precisely the impact it might have had, but we urge all our users to upgrade to Chamilo LMS 1.9.10 as soon as possible to avoid any problematic incidence.

Initial report: received by e-mail on 9/12/2014
Proper report: #7440
Fix: The fix is to upgrade to Chamilo LMS 1.9.10, released today. A standalone patch cannot be easily provided because it is too likely to break other parts of the code.
Affected versions: These vulnerabilities are likely to affect all previous versions of Chamilo LMS

If you are using **any** 1.9.x version of Chamilo, 1.9.10 is a minor version, so upgrading is **only** a matter of overwriting the current Chamilo code (removing the home/ directory in the **new** version package is recommended before you overwrite, in case you have a customized homepage).

If you would like to apply a patch manually (and although we **don't** have a complete and secure patch at the moment), you can use the 3 main changes that were applied to fix it. This might not be an exhaustive list and, as always, Chamilo or BeezNest are not responsible for what might happen to your platform (see the GNU/GPLv3 license for details):

- https://github.com/chamilo/chamilo-lms/commit/3463b0465f60e07ae03d41c6bd9fd8a8d030de4d
- https://github.com/chamilo/chamilo-lms/commit/e01f044d58a7698b44fdda3a73c83eb8181a4910
- https://github.com/chamilo/chamilo-lms/commit/28baec78d282baec9aaa2c85f4736921375c3f6a

Issue '#15' - 2014-08-25 - Moderate-high risk - SQL injection in mySpace/users.php

A security issue has been reported by NeoSys on our forum, which allows a person with access to a course's users tool to pass a specially-crafted "status" parameter to get more results than expected, and potentially access (and modify) other parts of the database.

This is considered moderate-high because it is limited to users having access to it, but because it as possibly high impact.

Initial report: http://www.chamilo.org/phpBB3/viewtopic.php?f=15&t=5443&p=23969#p23969
Proper report: #7242
Fix: (very easy one-liner) https://github.com/chamilo/chamilo-lms/commit/8a75f654066e4ff74567e5b427230117667325d1
Affected versions: this doesn't **seem** to affect versions of Chamilo LMS previous to 1.9.8.0, as this code was introduced recently, but please make sure you check your own installation to avoid any uncomfortable situation.
This patch will be included in release 1.9.8.3.

Issue '#14' - 2014-06-18 - Moderate risk - XSS vulnerability in online editor

A security issue has been published for FCKeditor very shortly after the release of Chamilo LMS 1.9.8. Considering we are including a vulnerable version of FCKeditor in our software, we cannot leave this issue unattended, and as such we are releasing Chamilo LMS 1.9.8.1, a patch version for 1.9.8, with just one file patched. See https://github.com/chamilo/chamilo-lms/commit/2b6686e620407ab8d4ceb8951de4ce978917fc93 for more details or if you want to apply the patch manually. This covers CVE-2014-4037.

Considering the relatively short period of time between the release of 1.9.8 and 1.9.8.1, we will still release 1.9.8.1 under the "commercial" name of 1.9.8, and will **link** all previous 1.9.8 links to the new 1.9.8.1 package. The changelog has been updated.
Considering you will be updating to 1.9.8.1 anyway, you'll notice that we've added a few (around 5) minor (mostly visual) issues that we caught just after the release of 1.9.8. So you kill 2 birds with one stone.

As always, being a minor version, you can just overwrite your previous installation with the files from this new package.

Issue '#13' - 2014-05-06 - Moderate risk - XSS vulnerability in user profile fields

Javier Bloem, independent white hat hacker from Venezuela, reported multiple possible attack vectors in description fields of Chamilo. Although these attacks require at minimum an access as a registered user to the portal, they do represent a vulnerability for those portals that are accepting open registration.

Patches have been commited to Github as commits:

- https://github.com/chamilo/chamilo-lms/commit/94706d7f99f7cb563c2a4f201c016caf7589fce1
- https://github.com/chamilo/chamilo-lms/commit/dd9bcd64fee588637914eec529cb489a8e89f2df
- https://github.com/chamilo/chamilo-lms/commit/a22589a9b909b32c89fe532d07b621d84b77fb34

Please update your portal(s) if you are in this case.
The fix is available in Chamilo 1.9.8 starting from Beta 1.

Issue '#12' - 2014-03-05 - High risk - File injection through FCKEditor

Eric Marguin, from agence-codecouleurs.fr, reported an attack related to flaw ~~#11~~, confirming it at the same time, whereby a skilled attacker injected a php file through an unprotected entry point in our implementation of FCKEditor.

Affected versions: 1.8.*, 1.9.*

To fix, please update files:

```
main/inc/lib/fckeditor/editor/plugins/ImageManager/config.inc.php
main/inc/lib/fckeditor/editor/plugins/MP3/fck_mp3.php
```

by adding the following line after the global.inc.php call.

```
api_block_anonymous_users();
```

Note that this issue, together with issue ~~#11~~, are fixed from 1.9.8 onwards.

Issue '#11' - 2013-12-09 - High risk - File injection through FCKEditor - CONFIRMED

Stijn Michels, one of Chamilo LMS users, reportes in #6860, that he has been attacked through a likely flaw in one of FCKEditor's plugins used in Chamilo LMS, through the fact that it is not checking identification from the user before uploading a file. The attack could not be reproduced. However, we think that preventive correction is important, and we have worked together to publish a patch that can be applied to any 1.8 or 1.9 version of Chamilo.

Affected versions: 1.8.*, 1.9.*

To fix, please update your main/inc/lib/fckeditor/editor/plugins/ajaxfilemanager/inc/config.php file adding the following on line 19:

```
api_block_anonymous_users();
```

and main/inc/lib/fckeditor/editor/filemanager/connectors/php/config.php to add

```
// Disabling access for anonymous users.
api_block_anonymous_users();
```

Issue '#10' - 2013-11-06 - Moderate risk - SQL Injection in specific:

(unrecommended case to add the following on lines 33 and 34)

High-Tech Bridge reported an SQL-injection-type security flaw in version 1.9.6 of Chamilo LMS (which also affects previous versions).
This flaw **only affect** Chamilo LMS platforms which use non-encrypted passwords mode (a mode that is available as a non-default option only during Chamilo LMS's installation process and is difficult to change afterwards).
If non-encrypted mode is selected (voluntarily) **and** malicious users have access to the profile edition form (which requires an active registered user account on the platform), then this issue represents a very high risk for you!
We believe and hope that most of our platform administrators have chosen the default recommended encrypted mode on their platform, but it is important to us to cover all risks. This is why we will be issuing a fix very shortly.

As a very quick fix, you can just open main/auth/profile.php, go to line 366 (function check_user_password()) and transform the following line:

```
$password = api_get_encrypted_password($password);
```

into this:

```
$password = Database::escape_string(api_get_encrypted_password($password));
```

This vulnerability has been assigned CVE-2013-6787.

See https://www.htbridge.com/advisory/HTB23182 for the original official report.

Issue '#9' - 2013-08-10 - Low risk - XSS in course title

Javier Bloem from Venezuela reported (through the Venezuela local group) one XSS flaw, involving the edition of a course title. This was fixed in commit https://github.com/chamilo/chamilo-lms/commit/3c770c201dbe1ce96480a3e51ff25d0b70c83514 (you can update a 1.9.* install just by using the file at https://raw.github.com/chamilo/chamilo-lms/3c770c201dbe1ce96480a3e51ff25d0b70c83514/main/course_info/infocours.php).
This flaw is considered "low risk" because it is an XSS (so stealing sessions is the kind of risk you get) **and** it is only accessible if you have the permission to create and edit courses, which you only get if you're a teacher.
It is, however, duly considered as flaw, as the default Chamilo installation **does** allow anybody to create a new teacher user, so it does represent a security risk for all people NOT READING the many recommendations on disabling this possibility as soon as they enter production.

Download the main/course_info/infocours.php script and replace it in your 1.9 installation from here: https://raw.github.com/chamilo/chamilo-lms/3c770c201dbe1ce96480a3e51ff25d0b70c83514/main/course_info/infocours.php

Issue '#8' - 2013-03-04 - Moderate risk - Several moderate security flaws

Fernando Muñoz, via Secunia SVCRP., kindly reported 3 flaws through Secunia, affecting at least version 1.9.4 (and most probably all previous versions) of Chamilo LMS.

In order to ensure maximum responsivity of our Chamilo administrators around the world, we provide 2 fix mechanisms that we give here by order of increasing level of required skills. We should be publishing 1.9.6 soon, which will include this fix. The patches below are provided for

version 1.9.4. You can find the details of the changes here: http://code.google.com/p/chamilo/source/detail?r=c9e8a27f8cde1f04dbe69d3f52a2e34c422bd679&name=1.9.x&repo=classic

- Download and apply the files replacement provided here: http://support.chamilo.org/attachments/download/3997/chamilo-1.9.4-vuln-8.zip Put the file directly into the root directory of Chamilo and uncompress there.
- Apply the patch provided here:
  For 1.9.4 http://support.chamilo.org/attachments/download/3999/chamilo-1.9.4-vuln-8.patch
  For 1.9.2 and 1.9.0 http://support.chamilo.org/attachments/download/4007/chamilo-1.9.2-vuln-8.patch
  For 1.8.8.6 http://support.chamilo.org/attachments/download/4008/chamilo-1.8.8.6-vuln-8.patch
  For 1.8.8.2 http://support.chamilo.org/attachments/download/4013/chamilo-1.8.8.2-vuln-8.patch
  For 1.8.7.1 http://support.chamilo.org/attachments/download/4014/chamilo-1.8.7.1-vuln-8.patch

If you require special assistance, please contact providers@chamilo.org to hire an expert, or ask for help on the forum: http://www.chamilo.org/forum

Issue '#7' - 2012-07-16 - Moderate risk - Several moderate security flaws

Fernando Muñoz kindly reported a series of moderate security flaws in Chamilo 1.8.8.4 (most likely also affecting all previous versions), of two XSS risks and one unauthorized file deletion risk. This has been registered in private task #5202.

In order to ensure maximum responsivity of our Chamilo administrators around the world, we provide 3 fix mechanisms that we give here by order of increasing level of required skills:

- Download and apply the files replacement provided here: http://support.chamilo.org/attachments/download/2864/patch-1.8.8.6.tgz Put the file directly into the root directory of Chamilo and uncompress there.
- Download version 1.8.8.6 and follow the normal upgrade procedure: http://code.google.com/p/chamilo/downloads/detail?name=chamilo-1.8.8.6.tar.gz&can=2&q=
- Apply the patch provided here: http://support.chamilo.org/attachments/download/2863/chamilo-1.8.8.4-to-1.8.8.6.patch

We considered the report was sufficiently serious for us to publish a new minor version of the software. Please apply using one of the three methods above AS SOON AS POSSIBLE.

Issue '#6" - 2011-06-15 - High risk - Several security flaws

Petr Skoda (<security *at* skodak *dot* org>) recently reported a series of flaws in Chamilo 1.8.8.2, which have been duly reported here http://support.chamilo.org/issues/3600 and here http://support.chamilo.org/issues/3601 and fixed in prevision for a special corrective 1.8.8.4 release within a few days (probably on the 18th of June). This release will come together with a series of improvements to the code and no upgrade procedure needed.
Patches are already available here:

- http://code.google.com/p/chamilo/source/detail?r=9ab36506b7099d29c005f4d4860a600e6734c166&repo=classic
- http://code.google.com/p/chamilo/source/detail?r=2b9e225f1659d253a8e458dabea5b71e4b57ac9b&repo=classic
- http://code.google.com/p/chamilo/source/detail?r=eef0cf45ceb4da084b3c61651fefae61d4e49fe2&repo=classic
- http://code.google.com/p/chamilo/source/detail?r=7ccba74a526d52c7831781e05ed52311439cf922&repo=classic

Issue '#5' - 2011-01-31 - High risk - Filesystem traversal flaw

Fernando Muñoz kindly reported a major security flaw in the document system, by which a user could gain access to the database on lightly-hearted configured servers.

- To fix it, please replace the changes found at
  http://code.google.com/p/chamilo/source/browse/main/document/download.php?spec=svn.classic.3c071b2b6555552651a9617b1c92a9a983da875f&repo=classic&r=3c071b2b6555552651a9617b1c92a9a983da875f
  and
  http://code.google.com/p/chamilo/source/detail?r=f2254d813f3a44a0a1b1717876b3c81df72a6879&repo=classic

- To discuss, please connect to http://support.chamilo.org/issues/2722

This flaw is being reported to our Twitter security account and to our mailing-list security@lists.chamilo.org
The fix will be included in Chamilo 1.8.8, to be released within 14 days, but we recommend applying the patch to any production system straight away.

Issue '#4' - 2011-01-28 - High risk - Filesystem traversal flaw

Fernando Muñoz kindly reported a major security flaw in the gradebook system, by which a user could gain access to the database on lightly-hearted configured servers.

- To fix it, please apply the changes found at http://code.google.com/p/chamilo/source/detail?r=b81c9c8012fa414d246a973aafddbde305c6f6f7&repo=classic
- To discuss, please connect to http://support.chamilo.org/issues/2705

This flaw is being reported to our Twitter security account and to our mailing-list security@lists.chamilo.org
The fix will be included in Chamilo 1.8.8, to be released within 14 days, but we recommend applying the patch to any production system straight away.

Issue '#3' - 2010-12-09 - Low risk - Wiki and core weaknesses in specific configurations

develop-it.be kindly scanned Chamilo 1.8.8 development version and found several minor issues, which we have fixed and included in 1.8.8 (to be released February 2011)

Issue '#2' - 2010-09-29 - High risk - Course directory removal risk through tasks tool

At around 11:55, Belgian time, on 29/09/2010, a new security issue has been reported by user mdube on the Chamilo forum.

- Risk level: high
- Versions affected: **1.8.6.2, 1.8.7, 1.8.7.1**
- Triggered by: teachers and administrators (no anonymous/student access)
- Patch: See patch

This security issue's risk level is considered **high** (on a scale of critical, high, moderate and low) in the sense you require edition permissions in the course to provoke it (relatively safe) but it provokes highly painful damages: it deletes a course directory, entirely.

This bug affects versions 1.8.6.2, 1.8.7 and 1.8.7.1.

At 21:00, Belgian time (less than 12 hours later), Julio Montoya, on behalf of BeezNest, developed a patch that you can download as a file and apply to your Chamilo 1.8.7.1 portal.

For previous versions of Chamilo, you will have to look at the patch and apply the differences manually. Suggestions are provided below:

- replacement work.php for 1.8.6.2
- replacement work.php for 1.8.7

The problem can be reproduced by trying to delete an un-existing student work from a course. The delete URL can be crafted manually, but it can also be triggered by a double click on the delete icon for a student work.
This means that if you have teachers accidentally double-clicking on the delete icon, they can delete the entire course directory. The only solution then is to restore the course directory quickly from your daily backup.

This bug was introduced in November of 2009, while still working on Dok€os, by a then member of the BeezNest team trying to fix a complex issue by using the permanently_remove_deleted_files parameter to decide whether to delete the files permanently or to leave them on disk. This flaw could apply to Dok€os 2.0 (cannot be checked until the code is made available). The developer doesn't work with us anymore, and we have considerably improved the review process, but this specific kind of bug implies a peer review process, and this can only come with regular investment.

Using the services of an official Chamilo provider guarantees your contributions go to Chamilo and help many other organizations and people around the world, just as
you benefit from contributions from many others. Contribute to the Chamilo project using our official providers services and encourage our healthy and socially responsible economical model!

Best regards,

Yannick Warnier
Lead developer for Chamilo 1.8

Issue '#1' - 2010-08-02 - Wiki issues

Fixed in 1.8.7.1 package.

Updated by Yannick Warnier about 2 months ago · 125 revisions