Recovery of the access from the Internet to the CMS

We are contacting you in relation to your website.

As you probably are aware, following a security incident and based on clear instructions from DIGIT S (CSIRC) and HR-DS security colleagues, we have blocked editorial access from the internet to all Drupal 7 websites on 17th April.

We are now happy to inform you that we have implemented a set of security measures to that have permitted us to reactivate editorial access from the internet. The opening of these services take place on a priority site-by-site basis. We have launched a first batch of highly impacted websites from DGs like SCIC, ESTAT, EEAS or TAXUD, for which we are already working on restoring internet access for authenticated users.

As a first step, we have sent a request to change/create the registration of the application in EU Login – the objective is to have it activated for using Adaptive Security, a new feature of EU Login which forces the use of 2FA for users connecting from the internet while maintaining password only for users connecting from the internal EC network (similar to RCAM access). As soon as this is in place and we have validated it is functioning correctly, we will start the implementation of the remaining set of remediation and additional security controls to ensure correct functionality for your site (only those having a direct business impact are indicated in the table below – additional ones, such as redeployment of code, clean up, firewall new rules, additional monitoring or similar are not included):

Item	Description	Expected business impact
1.	Activation of Adaptive Security for all users	All users connecting from the internet will have to use 2FA authentication, while users connecting from the internal EC network will continue to use their password only (similar to RCAM). Any user not already having the 2FA activated will need to activate 2FA (possible as a self-service for self-registered users). 2FA is best achieved by using the EU Login app – you can find more information on the procedure in the attached user documentation for EU Login (Install and initialise the EU Login Mobile App section on page 12) since it does not require a phone number of the user. Successively, authentication will be done using the EU Login app (sections Sign in with an EU Login account using the EU Login Mobile App PIN code, Sign in with an EU Login account using the EU Login Mobile App QR code, Sign in with an EU Login account using On Mobile authentication sections respectively on pages 5,6 and 9). Please be aware that due to the high impact on the site owners, we started the process for the reactivation of your site without having yet a dedicated communication sent to the users, but the technical information is included in the attached manual. An improved version might be prepared in the next days and COMM colleagues will share with you if this will be the case.
2.	Removal of administrator rights for all users currently having such rights, with reactivation in the future following a centrally managed process (still to be defined).	Users having administrator level access will no longer have such access rights. For certain operations where previously an administrator user was used it might be necessary to ask for COMM EUROPA MANAGEMENT support or to implement code for creating new roles with the desired access rights (roles permissions changes in production will no longer be possible and any change to the roles permissions will have to be submitted as code through the regular Quality Assurance process).
3.	Certain high-risk access permissions will be removed from all existing roles – such permissions are considered security sensitive and should be handled with particular attention.	It will no longer be possible for any of the existing roles to execute certain operations (administer content types/fields/filters/views and similar in production, change themes, administer permissions and users, change some site configuration data, bypass access rights, work with features in production or use PHP code directly). For some of the access rights (specifically administer users) a solution will be envisaged in the next weeks while for the rest the only allowed alternative will be delivered through code passing through the regular QA process.
4.	All new users will be inactive by default and activation by user management will be necessary. This will be in place both for new Drupal and new EU Login users.	New users need to be activated after creation by a user with sufficient rights. Until a procedure is defined and implemented, you will be required to contact CEM for activation of such users.

5.	Users that were not active in the past 12 months or have never logged in will be deactivated. Similarly, all new users created after 25 March 2020 will be deactivated.	All those users will have to be reactivated if they need access.
6.	Changes to the default usernames created with each Next Europa instance – if you were using the fpfis_admin, user_administrator, user_contributor or user_editor they will no longer be available. We will no longer allow for generic users which can be shared by multiple persons and each person will be required to use their individual credentials.	limited impact on persons using any of the above 4 users or similar generic ones created in the past.
7.	Full clean-up of any possible remaining (will be done for safety on all sites, even if for your site no trace of security breaches were detected).	Short downtime for the site when reactivating the site (similar to a deployment).

As indicated earlier, a solution for the user management is still under review in order to allow users activation and roles assignment directly by you, but until such a solution is in place you may need to request CEM support for such operations. For other restricted operations, you will need to include changes previously done directly in production into a code delivery passing through QA validation to ensure proper security remains in place.

Please do not hesitate to get back to us in case you need further details. We will let you know as soon as we will be ready to proceed with the process for the reactivation.

DG COMM

Documents

- 📄 EU_Login_Tutorial.pdf (1,0 Mb)

If you have any comments, suggestions or questions concerning the content of this newsletter please write to europamanagement@ec.europa.eu. We will be pleased to provide additional information.

The European Commission is committed to personal data protection. Any personal data is processed in line with the Regulation (EU) 2018/1725. Please read the privacy statement