Sage X3

Security Alert – ADMCA & ECOMM FAQ

This document contains FAQs for Colleagues, Partners and Customers related to a Sage X3 security alert. Please note, this document may be update periodically so we recommend you check for the latest copy.

Table of Contents

Frequently Asked Questions

Risk

What is the issue?

This alert relates to two generic users (ADMCA and ECOMM) that have been supplied by default when installing Sage X3 Version 11 and Sage X3 Version 12 for demo purposes. In some rare cases, when Sage X3 Security Best Practices have not been followed, there might be an access path to administration functions on production sites by an elevation of privilege.

This issue has been reported on some environments, thus Sage strongly advises that customers that have been first installed on Sage X3 Version 11 and Sage X3 Version 12, to implement the steps below to mitigate this completely.

Does this issue impact Sage X3, and who does it affect?

Yes, these generic users are created by default regardless of implementation of Sage X3.

If Sage X3 Security Best Practices have been followed this should mitigate exposure to this risk, but please read on to see if you need to take action.

Which versions of Sage X3 does this impact?

This impacts customers with a first installation of Sage X3 Version 11 and Sage X3 Version 12 before release 2019 R2 or who upgraded from a previous version to those releases (even if the customer has subsequently upgraded to a more recent release).

Does this impact all kinds of authentication?

As per our Sage X3 Security Best Practices, if you use an externalized authentication methods (such as LDAP, Oauth2), **there is no risk**, related to this alert.

However, if you use the legacy DB authentication, and if the user ADMCA and/or ECOMM exists with its default password, therefore, the solution outlined below will need to be taken.

What is the nature of this risk?

ADMCA and ECOMM users allow a connection to an account and could potentially access other production environments through privilege elevation.

What if I do have a public URL, is there a risk for me?

If you have a public URL, you are at risk of having somebody accessing your site using ADMCA or ECOMM with the knowledge of security breach to exercise the elevation of privileges and access to your data. Please follow the steps below to mitigate this risk.

What if I don't have a public URL, is there a risk for me?

With a private URL, the risk is restricted to internal people accessing data, where a colleague could access ADMCA/ECOMM and elevate rights to access production.

Are there any other considerations for this risk?

By following best practices and securing your URL or not making your URL publicly available, you protect yourself against external risk. Note – this does not suggest that there may not be an internal risk.

I'm a cloud customer of Sage, am I at risk?

Cloud customers of Sage (MT, ST, SSC, SA Cloud Instance) are not at risk, as best practices have been followed.

Solution:

What should I do to eliminate this risk?

If you cannot immediately use the patch, check whether you have ADMCA and/or ECOMM users; if these are present in your X3 instance, then implement the below steps:

Sage recommends to immediately to the following manual steps to eliminate the risk:

- Deactivate or delete ADMCA and ECOMM users if you are not using them.
- If you use them, and if you use the DB authentication, make sure their default passwords have been changed, so these accounts cannot be used with a default weak password (if they are not in DB authentication, there is no risk). If you use ATP, check if the default ADMCA user managed in the scripts has been changed. If not, change the password of ADMCA rather than deactivating it so you won't block ATP.
- There is also, in the configuration file (nodelocal.js), a parameter that should be set to avoid the ability to perform a privilege elevation once connected with ADMCA. This parameter, called *adminUserRestrict* and documented in the best practices document, prevents the risk if it is set to *true*. You can find out how to do this in this FAQ.

In addition, Sage has published a patch for V11 and V12:

This patch, **available from the 27 October 2022**, delivers a simple tool to install on the server and to run once. This tool will check if ADMCA and ECOMM are present, if they are in DB authentication, and if they still have their default password set. If this is the case, these accounts will automatically be deactivated. The tool will also add the *adminUserRestrict* parameter in the nodelocal.js file with the right value. The patch is delivered with a documentation that explains how to proceed.

Note that:

- running this patch doesn't require to stop the Syracuse server (ADMCA / ECOMM users will be deactivated, the privilege escalation will only be impossible at the next Syracuse startup).
- Change the default password of ADMCA prior to run the utility if you use it to avoid blocking connections based on it (check if it is used for ATP scenarios if you use ATP).

The tool will also display additional warning about potential security issues such as weak passwords. Carefully check the messages that will display when running it and apply the recommendations.

Taking all the above actions completely eliminates this risk, related to this alert.

The next V12 release (2022 R4) will include this fix:

The next release of V12 (2022 R4) will integrate a new release of Syracuse (12.17.0) that will trigger the deactivation of ADMCA and ECOMM at startup time if the passwords weren't modified and if they use a DB authentication. It will also consider the *adminUserRestrict* parameter to set to *true* by default.

How do I manually deactivate the ADMCA and/or ECOMM user?

Steps:

- Connect on Sage X3 as admin
- Go to the Administration / Users / Users function
- select the account ADMCA if it exists (if not, there is no issue).
- Once the record is selected, click on *Edit*, make sure the *Active* checkbox is deactivated, and click on the *Save* button.

As an addition to the previous step, you should edit the nodelocal.js configuration file located on the server to add the parameter *adminUserRestrict* with a value set to true. This will prevent any further escalation of privileges.

If I have followed the steps above, do I need to still install the patch?

If you have taken the above steps, then you will have eliminated the risk. However, to follow Sage X3 Security Best Practices, we always recommend you apply the latest security patches.

Where can I find the security best practices for Sage X3?

Sage X3 security best practices are freely available on Sage X3 online help.

Where can I get more information going forward?

Should you need any further information, please reach out to your Partner Account Manager.

sage.com