Auditdata
Support Bulletin

| Support Bulletin details			
Title:	Support bulletin	**Support Bulletin #**	DN02551/04
Product:	Auditbase	**Date:**	25/03/2025
Reason for Action:	Information from HIMSA site - Noah 4.16 provides an important security update.	**Author:**	Mark Crawshaw
Information Classification:	Public	**Status:**	Approved

Description
Issue:

https://www.himsa.com/news/noah-4-16-release-with-important-security-update-for-noah-4-ic/
On March 12, 2025, HIMSA released Noah System 4.16. Noah 4.16 provides an important security update, and HIMSA recommends that all installations be upgraded to Noah 4.16 as soon as possible. For Noah business systems such as Auditbase this must be done via the supplier, Auditdata's, update path, not via the path described for Noah System on the HIMSA website.

According to the information we have received, HIMSA is not aware that the vulnerability has been exploited but is treating this issue with the highest priority.

For questions related to the identified vulnerability or to the Noah 4 changes, please contact HIMSA directly. You can find HIMSA's contact information here: HIMSA website

| **Solution:** |

Recommended Actions

To maintain system security and ensure continued compatibility, we strongly recommend the following steps:

1. Enhance firewall security:

    ο While awaiting Auditdata's official releases supporting Noah 4.16, please review and update your firewall settings on each PC that uses Auditdata solutions according to the procedure described below.

    ο Remove or disable any inbound rules associated with NoahServerService to ensure Noah runs in a more secure, local-only mode.

2. Hotfix or upgrade to the latest versions of Auditdata software:

    ο We will provide download instructions once implementation and thorough testing is complete.

Updating firewall settings

It is possible to quickly reduce the impact of this vulnerability by disabling the firewall rules that were activated during the NOAH 4 installation. While this measure does not fully mitigate the vulnerability, it significantly lowers the associated risk.
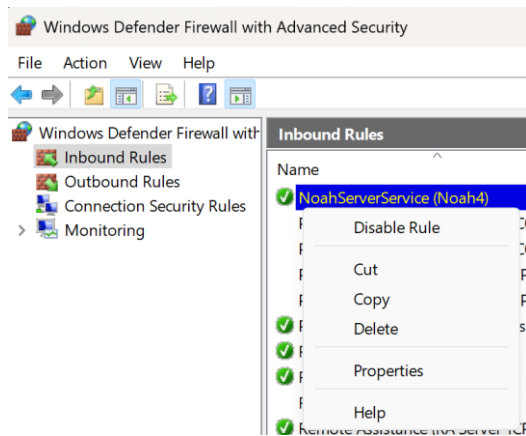
We therefore recommend the following precautionary measure to enhance the security of your PC. To adjust your firewall configuration, accordingly, please follow these instructions:

1. Open a Run window (Win+R). At the command prompt, type: wf.msc
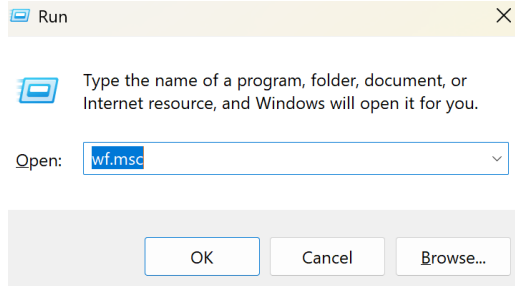
2. In the Inbound rules find NoahServerService (Noah4) rule and disable it

3. These rules can also be applied centrally by IT departments utilizing:
   a. Group Policy
   b. Microsoft Intune.
   c. Microsoft Endpoint Manager.
   d. PowerShell

Auditbase and Noah update

It is not possible for customers to update Noah within Auditbase themselves due to incompatibility of Noah 4.16 with earlier versions of Auditbase. Auditbase is designed, tested and certified by HIMSA around only one specific version of Noah. That version is not interchangeable. You must contact Auditdata for either a hotfix or an upgrade.

Auditdata will include Noah 4.16 in the upcoming version of Auditbase 6.8.0 due for release currently in Easter week. Where possible, we also plan to provide a hotfix for some of the earlier versions of Auditbase .

If you are using the following Auditbase versions, you should contact support@auditdata.com to arrange for a hotfix.

- Auditbase 6.2.0.x
- Auditbase 6.3.0.x
- Auditbase 6.4.0.x

- Auditbase 6.5.0.x
- Auditbase 6.6.0.x
- Auditbase 6.7.0.x

Important Notes

Due to the complexity of the issue, a hot-fix from HIMSA for existing or previously released Noah versions is not possible. Updating to Noah 4.16 (via an Auditbase hotfix or upgrade) or changing firewall settings is the only effective way to address the vulnerability.

Support and Assistance

If you need assistance with Auditdata software or have any concerns, our support team is ready to help. You can contact us by sending an email to: support@auditdata.com