



## Project

Tue. 21st April, 2026

# TYPO3-CORE-SA-2026-005: Cleartext storage of Backend User Passwords

Categories: [Development](#), [TYPO3 CMS](#)

Created by Oliver Hader

It has been discovered that TYPO3 CMS is susceptible to sensitive data exposure.

- 
- **Component Type:** TYPO3 CMS
  - **Subcomponent:** User Profile Settings (ext:backend)
  - **Release Date:** April 21, 2026
  - **Vulnerability Type:** Sensitive Data Exposure
  - **Affected Versions:** 14.2.0
  - **Severity:** High
  - **Suggested CVSS:**  
[CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:H/VI:N/VA:N/SC:H/SI:H/SA:H](#)
  - **References:** [CVE-2026-6553](#), [CWE-312](#)
- 

## Problem Description

The backend user settings module (*SetupModuleController*) incorrectly conflates entity data (like passwords or email address) with user-interface settings (like theme, display options) when persisting changes. As a result, passwords were stored in cleartext in the *uc* and *user\_settings* fields of the *be\_users* database table.

The cleartext data was only persisted if users changed their credentials in the backend user settings module when the TYPO3 14.2.0 release was used (not in any other version).

## Solution

Update to TYPO3 version 14.3.0 LTS that fixes the problem described.

### Manual actions required

Updating to the patched release does not retroactively clean existing data. It is recommended to execute all **User Settings** upgrade wizards in the TYPO3 Install Tool, including the dedicated **User Settings Scrubbing** wizard, which sanitizes the incorrectly persisted cleartext values from the *uc* and *user\_settings* fields of the *be\_users* table. **Additionally, affected backend user accounts should be assigned new passwords.**

Admin Tools → Upgrade → Upgrade Wizard → User Settings Scrubbing

## Credits

Thanks to Martin Clewing for reporting this issue, and to TYPO3 core team members Oliver Hader, Stefan Bürk and Garvin Hicking for fixing it.

## General Advice

Follow the recommendations that are given in the [TYPO3 Security Guide](#). Please subscribe to the [typo3-announce](#) mailing list.

## General Note

All security-related code changes are tagged so you can easily look them up in our [review system](#).



**Project**

**TYPO3 Association**

- Members & Membership
- Funding & Finances
- Structure
- By-Laws
- Strategy
- Contact

**TYPO3 Company**

- Structure & Leadership
- Contact

**Governance & Values**

- Vision, Mission, and Purpose
- Community Values
- Decision-Making
- Security
- Data Privacy
- Rules, Guidelines, & Policies

**Strategic Collaboration**

- eco — Association of the Internet industry
- Open Source Business Alliance (OSBA)
- Open Source Initiative (OSI)
- Open Website Alliance (OWA)

**TYPO3 Universe**

**TYPO3**

- TYPO3 CMS
- Case Studies

**Community**

- Community
- Meet

[Products & Services](#)

[Get help](#)

[Solutions](#)

[Contribute](#)

[Partners](#)

### News & Events

[News & Events Hub](#)

[Events](#)

[Newsletter](#)

### More

[Extensions](#)

[Documentation](#)

[My TYPO3](#)


[Get TYPO3](#)


### Get in Touch


 [LinkedIn](#)

 [Instagram](#)

 [Bluesky](#)

 [Mastodon](#)

 [Facebook](#)

 [YouTube](#)

---

© 2026 TYPO3 Association.

[Legal Notice](#)

[Privacy Policy](#)



Open. Sustainable. A Digital Public Good.