# Security Assessment Report Sunet Drive 2024-04

## MFAZones and StepUp Auth

Jonas Lejon, Anton Linné, Jesper Larsson

2024-04-29
Report version 1.1

## Index

Security Assessment Report Sunet Drive 2024-04
- Index
- Introduction
- Severity Glossary
- Test Methodology
  - White-box audit against Sunet Drive
- WP1 - Identified Vulnerabilities
- Conclusions

## Introduction

Sunet has enlisted Triop to assess the security of certain parts of its NextCloud implementation. This audit focuses on Step-up authentication and MFA Zones.

This report is one of three reports. The other two reports are:

- Everything related to Sunet Drive
- Backup

## Scope

- **Work Packages**
  - WP1 - MFA Zones and StepUp Authentication
- **Deadline:**
  - 22.05.2024

## Severity Glossary

The following section details the varying severity levels assigned to the issues discovered in this report.

***Critical***: The highest possible severity level. Categorizes issues that allow attackers to achieve extensive access to sensitive areas, such as critical systems, applications, data or other pertinent components in scope.

*High*: Categorizes issues that allow attackers to achieve limited access to sensitive areas in scope. This also includes issues with limited exploitability that can facilitate a significant impact upon the target in scope.

*Medium*: Categorizes issues that do not incur major impact on the areas in scope. Additionally, issues requiring a more limited exploitation are graded as *Medium*.

*Low*: Categorizes issues that have a highly limited impact on the areas in scope. Mostly does not depend on the level of exploitation but rather on the minor severity of obtainable information or lower grade of damage targeting the areas in scope.

*Info*: Categorizes issues considered merely informational in nature. They are mostly considered as hardening recommendations or improvements that can generally enhance the security posture of the areas in scope.

## Test Methodology

This section describes the testing methods used by Triop for this project and details the coverage achieved. It offers an analysis of the different components examined within the scope. Moreover, it provides additional details about the areas that underwent a thorough evaluation to address the absence of significant security vulnerabilities despite the comprehensive reviews conducted by the audit team.

### White-box audit against Sunet Drive

As part of the penetration testing assignment, the focus was on evaluating the security effectiveness of the MFA Zone and Step Up Auth plugins developed by Sunet. The testing aimed to identify possible methods to bypass the MFA requirements and access secured files. The testing approach included:

- Utilizing OAuth tokens to attempt access through different API endpoints, examining the enforcement of MFA protocols under various authentication scenarios.
- Employing session cookies in conjunction with different API endpoints to determine if an established session could override MFA protections.
- Testing the implementation of WebDAV commands, exploring both the standard operations and those that might expose vulnerabilities in the MFA implementation.
- Attempting access with users from the same tenant as well as cross-tenant users to check for inconsistencies or oversights in multi-tenancy environments that could allow unauthorized file access.
- Accessing functions or features which should be disabled as admin or regular user

Further investigations during the penetration testing focused on ensuring the integrity of the MFA system under various conditions. We conducted tests to verify that MFA protections could not be bypassed using any known vulnerabilities or unconventional methods, encompassing both direct attacks on the MFA mechanism and indirect approaches that might sidestep the need for secondary authentication. Particular attention was given to the functionality and security of MFA backup codes, confirming their proper invalidation after a single use which aligns with security best practices and prevents potential misuse.

Additionally, we reviewed common user actions such as login, registration, and password reset processes. This phase of testing looked for typical vulnerabilities within these functions, including injection attacks, improper session handling, and flaws in input validation. The aim was to ensure that the MFA system remained secure not only in preventing direct unauthorized access but also in safeguarding against vulnerabilities in associated user interaction workflows.

## WP1 - Identified Vulnerabilities

The following sections list both vulnerabilities and implementation issues spotted during the testing period. Note that findings are listed in chronological order rather than by their degree of severity and impact. The aforementioned severity rank is simply given in brackets following the title heading for each vulnerability. Each vulnerability is additionally given a unique identifier (e.g. *SUN-01-001*) for the purpose of facilitating any future follow-up correspondence.

No vulnerabilities was identified related to MFAZones and Step Up authentication.

## Conclusions

The auditors tried to bypass MFA and Step-up authentication but failed. So, even though the efforts were made, our conclusion is that the quality is outstanding regarding the main target of the audit.

Triop would like to thank Anders, Richard, Magnus and Micke from the Sunet team for their excellent project coordination, support and assistance, both before and during this assignment.