Security Assessment Report Sunet Drive 2024-04

Jonas Lejon, Anton Linné, Jesper Larsson

Backup

2024-05-08
Report version 1.1

Index

Introduction

Sunet has enlisted Triop for a security assessment of certain parts of its NextCloud implementation. This audit focuses on a soft audit of the backup procedures and how/if ransomware attacks could affect the backups.

Scope

- **Work Packages**
  - WP2 - Backup
- **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.

No vulnerabilities was found within the backup-scope.

WP2 - Backup

As the backup system audit is a soft audit, no active tests have been conducted in this work package. Sunet and the auditors answered the questions via e-mail, and follow-up questions were answered.

Documentation has also been used as input for the recommendations below.
One of Sunet's main concerns was that ransomware could encrypt all or parts of the backup and exfiltrate information. No vulnerabilities have been identified, but only recommendations have been made.

Backup recommendations

It is crucial that Sunet adopts the 3-2-1 backup strategy, a widely recognized and recommended approach by NIST and others, to ensure the security and recoverability of its data.
The 3-2-1 backup strategy states that you should have 3 copies of your data (your production data and 2 backup copies) on two different media (disk and tape) with one copy off-site for disaster recovery.

Given our understanding that all backups are now based on the S3 technology, we strongly recommend the addition of another backup media to further enhance data security.

It is of utmost importance that Sunet reduces the number of ways to access the backup data, thereby significantly enhancing the system's security. We also recommend adding at least two layers of protection for each way of accessing backup files.

The current ways of accessing the backup data are:

1. Via SSH. Keys are in the hardware of the users and administrators
2. Via virtualisation layer, consol or similar
3. Via S3-keys
4. Physical access via hardware in the data centre
5. Via OOB management such as iLO or similar

Other recommendations include:

- Encrypt the backups, either the drives directly or individual backup files
- Use WORM storage. Includes non-rewriteable technology
- Audit (log) all access to backup files and follow up on the access

Conclusions

The conclusion of our work, including WP2, is that the overall security of the parts of Sunet Drive that we audited is good. We recommend a few things to change to make the security even better.

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.