Contents

[Nextcloud Security and Authentication Features 2](#_Toc146380985)

[Authentication Capabilities 2](#_Toc146380986)

[Control Over Data Flow 2](#_Toc146380987)

[Security in Development Processes 2](#_Toc146380988)

[Authentication Capabilities 2](#_Toc146380989)

[Encryption 2](#_Toc146380990)

[Other Features 2](#_Toc146380991)

[Observations for Nextcloud Configuration Files 3](#_Toc146380992)

[Nextcloud Installation Observations: 4](#_Toc146380993)

[Observations for Nextcloud Security Vulnerabilities: 4](#_Toc146380994)

[Recommendations: 6](#_Toc146380995)

[Vulnerability Trends Over Time: 6](#_Toc146380996)

[Vulnerabilities by Impact Types: 7](#_Toc146380997)

[Individual Contributions to the Team: 8](#_Toc146380998)

[Reflections: 9](#_Toc146380999)

[References: 10](#_Toc146381000)

## Nextcloud Security and Authentication Features

* File Access Control

## Authentication Capabilities

* LDAP/Active Directory
* Kerberos
* SSO/SML 2.0
* Two factor authentication

## Control Over Data Flow

* Logging and monitoring
* Permission
* Fine-grained File Access Control
* Encryption
* Virus Scanning
* Data Retention

## Security in Development Processes

* Training
* Requirements
* Implementation
* Verification
* Response

## Authentication Capabilities

* Rate Limiting
* Password Handling
* Brute Force Protection
* Password Handing
* Security Hardening
* Encryption Session Data

## Encryption

* Server-side Encryption
* Key Management,
* End to End Client-side Encryption

## Other Features

* Include root certificate
* Support for security headers by the web server
* Trusted domains
* Preventing directory traversals

## Observations for Nextcloud Configuration Files

Did not see the domain name in the registrar’s approval list. Solution verify domain name is in the approval list to prevent cybersquatting, a term used by bad actors to contact customers to phish for their information. Nextcloud uses http instead of https (s stands for security)

In the Database Configuration documentation, it references MySQL, Maria DB and PostgreSQL, I did not I did not see Oracle 19c (which is recommend) to install. Oracle 19c is widely used and is a preferred method for database capabilities.

[CVE-2023-23942 | SUSE](https://www.suse.com/security/cve/CVE-2023-23942.html)

Description based upon CVE-2023-23942:

The Nextcloud Desktop Client is a tool to synchronize files from a Nextcloud Server with your computer. Versions prior to 3.6.3 are missing sanitisation on qml labels which are used for basic HTML elements such as `strong`, `em` and `head` lines in the UI of the desktop client. The lack of sanitisation may allow for javascript injection.

Solution: It is highly recommended that the Nextcloud Desktop Client be upgraded to 3.6.3. There are no known workarounds for this issue.

List of Security Patch Names SUSE Package Hub 15 SP4 openSUSE-2023-90

SUSE Package Hub 15 SP5 openSUSE-2023-171

openSUSE Leap 15.4 openSUSE-2023-90

openSUSE Leap 15.5 openSUSE-2023-171

CVE-2021-29438

The Nextcloud dialogs library (npm package @nextcloud/dialogs) before 3.1.2 insufficiently escaped text input passed to a toast. If your application displays toasts with user-supplied input, this could lead to a XSS vulnerability. The vulnerability has been patched in version 3.1.2 If you need to display HTML in the toast, explicitly pass the `options.isHTML` config flag.

Published: 2021-04-13

Updated: 2021-04-19

Notes is a note-taking app for Nextcloud, an open-source cloud platform. Starting in version 4.4.0 and prior to version 4.8.0, when creating a note file with HTML, the content is rendered in the preview instead of the file being offered to download. Nextcloud Notes app version 4.8.0 contains a patch for the issue. No known workarounds are available.

CVE-2023-23942

he Nextcloud Desktop Client is a tool to synchronize files from a Nextcloud Server with your computer. Versions prior to 3.6.3 are missing sanitisation on qml labels which are used for basic HTML elements such as `strong`, `em` and `head` lines in the UI of the desktop client. The lack of sanitisation may allow for javascript injection. It is recommended that the Nextcloud Desktop Client is upgraded to 3.6.3. There are no known workarounds for this issue.

Remediation: Recommend upgrade Nextcloud Desktop Client to 3.6.3. There are no known workarounds for this issue. System requirements.

Webserver:

• Apache 2.4 with mod\_php or php-fpm (recommended)

• nginx with php-fpmWeb server configuration

• The recommended nginx configuration changed.

PHP Runtime

• 7.4 is no longer supported

• 8.0 (deprecated)

• 8.1 (is not recommended)

• 8.2 (recommended)

## Nextcloud Installation Observations:

Installation Issues going from 25.0.11 to 26 discussed in the nextcloud community. Users were not able to revert 26.0.2.1 back to 26.2.2 after upgrade installation. The users were also missing data after the upgrade. Based upon the nextcloud community, there was not a fix available at that particular time.

## Observations for Nextcloud Security Vulnerabilities:

Overall, there have been 271 security vulnerabilities files found in Next Cloud from 2016 to 2023. The security vulnerabilities can be found at: Nextcloud : Security vulnerabilities, CVEs (cvedetails.com). Here are examples of the vulnerabilities found in the Nextcloud software:

Nextcloud cross site scripting (XSS)

From 2016 to 2023, there were 33 cross site scripting (XSS) Nextcloud security vulnerabilities found. Two examples can be found on the following CVE website: Nextcloud : Security vulnerabilities, CVEs xss, cross site scripting (cvedetails.com).

There have been 66 Nextcloud security vulnerabilities by impact types from 2016 to 2023.

For example: Log4Shell CVE-2021-4422

CVE-2021-45046

It was found that the fix to address CVE-2021-44228 in Apache Log4j 2.15.0 was incomplete in certain nondefault configurations. This could allow attackers with control over Thread Context Map (MDC) input data when the logging configuration uses a non-default Pattern Layout with either a Context Lookup (for example, $${ctx:loginId}) or a Thread Context Map pattern (%X, %mdc, or %MDC) to craft malicious input data using a JNDI Lookup pattern resulting in an information leak and remote code execution in some environments and local code execution in all environments.

Log4j Shell Solution:

Log4j 2.16.0 (Java 8) and 2.12.2 (Java 7) fix this issue by removing support for message lookup patterns and disabling JNDI functionality by default

CVE2021**-**45105

CVE-2021-45105 is a remote code execution (RCE) vulnerability that enables malicious actors to execute arbitrary Java code, taking control of a target server.

Apache Log4j Shell versions 2.0-alpha1 through 2.16.0 (excluding 2.12.3 and 2.3.1) did not protect from uncontrolled recursion from self-referential lookups. This allows an attacker with control over Thread Context Map data to cause a denial of service when a crafted string is interpreted.

Mitigation:

This issue was fixed in Log4j 2.17.0, 2.12.3, and 2.3.1.

Nextcloud Security Vulnerability

Apache Log4j2 Remote Code Execution Vulnerability

CISA description:

Apache Log4j2 contains a vulnerability where JNDI features do not protect against attacker-controlled JNDI-related endpoints, allowing for remote code execution.

CVE-2021-44832

Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security releases 2.12.2, 2.12.3, and 2.3.1) JNDI features used in configuration, log messages, and parameters do not protect against attacker-controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. From log4j 2.15.0, this behavior has been disabled by default. From version 2.16.0 (along with 2.12.2, 2.12.3, and 2.3.1), this functionality has been completely removed. Note that this vulnerability is specific to log4j-core and does not affect log4net, log4cxx, or other Apache Logging Services projects.

Solution:

CISA required action:

For all affected software assets for which updates exist, the only acceptable remediation actions are: 1) Apply updates; OR 2) remove affected assets from agency networks.

## Recommendations:

I would also recommend other encryption methods in protecting consumer’s data. One data encryption example is Tripe Data Encryption Standard (DES). Triple DES is a symmetric encryption technique and more advanced of the Data Encryption Standard (DES).

I would also recommend both a public key and a private key. Symmetric keys are used to encrypt and decrypt data

Asymmetric keys use two keys: The public key is to decrypt data. The private key is used to decrypt data. This method is widely used in when sending and receiving emails.

Compliments to the Nexcloud developers for being the first vendor to implement End to End Client-side Encryption. This technique ensures neither nextcloud server nor any code provides (like in the browser) has ever access to the unencrypted data.

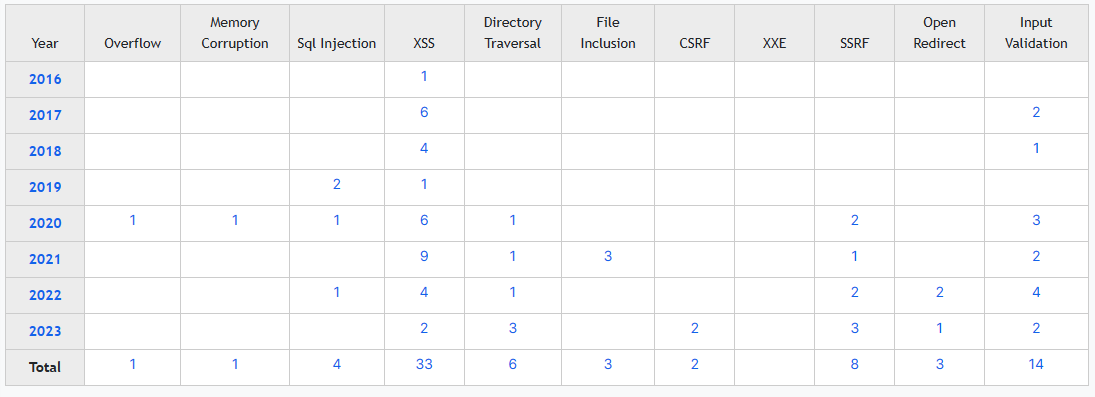
As part of the nextcloud maintenance schedule, patches should be applied on a quarterly basis to prevent vulnerabilities on the network.

The Log4jShell vulnerability affected both the private and public sector. Apache Log4j2 contains a vulnerability where JNDI features do not protect against attacker-controlled JNDI-related endpoints, allowing for remote code execution.

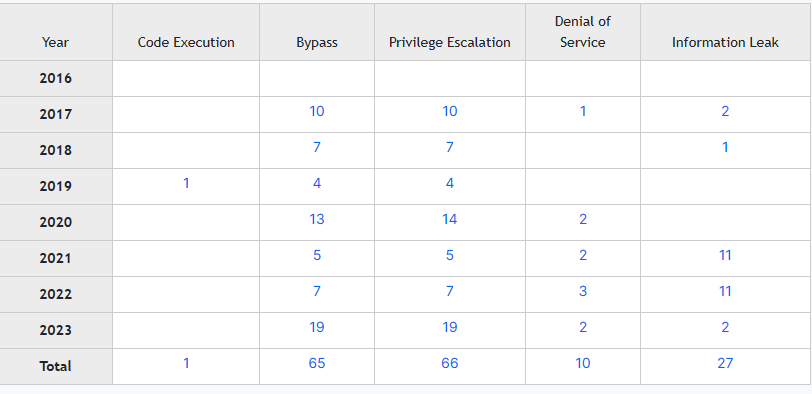
CISA Recommendation:

For all affected software assets for which updates exist, the only acceptable remediation actions are: 1) Apply updates; OR 2) remove affected assets from agency networks.

## Vulnerability Trends Over Time:



## Vulnerabilities by Impact Types:



\*\*These statistics are related to vulnerabilities of the nextcloud software. Please reference link at *Nextcloud : Products and Vulnerabilities*. <https://www.cvedetails.com/vendor/15913/Nextcloud.html> for further guidance.

## Individual Contributions to the Team:

Created the following NextCloud files in GitHub:

* Config file.md🡺Provided as sampling of nextcloud’s configuration file based upon nextcloud’s documentation. Provided recommendations on current vulnerabilities, missing patches, server upgrade, desktop clients, etc.
* Maintenance Release🡺Nextcloud release (pertains information on the next update, maintenance schedule and EOL version numbers). All information was based upon research conducted in Nextcloud’s documentation

Created Nextcloud security.md which consisted of the following:

* Identifying Nextcloud Security Policy🡺based upon research conducted
* Regulations, governance, compliance and policies based upon rules GFH Bank must follow🡺based upon research conducted
* Nextcloud Support Versions🡺based upon research conducted
* Vulnerabilities🡺Extensive research was performed to identify software vulnerabilities in Nextcloud. Provide comments, mitigations and fix actions for a well known vulnerability affecting both the private and public sector. There were 272 vulnerabilities associated with Nextcloud’s software. Provided a few examples of the vulnerability finding and made recommendations on how to mitigate those findings.
* Created two file types and provided analysis based upon trends over time and by impact type
* Created nextcloud system requirments.md file based upon nextcloud configuration files. Provided installation recommendations to install software based upon a user’s environment.
* Created a User System REquirments.md. Created this file based upon the customer’s environment. Typically, the software engineer would need to coordinate with the customer to understand the business environment when working in a Dev/SEC Ops environment
* Created Nextcloud Security Features.md file to provide details on the security features nextcloud currently has to offer their customers.
* Created a customer misuse case diagram. Originally, I started with a sysadmin diagram. Based upon a suggestion from a team members, I decided to scale back by creating a misuse case for a GFH Bank customer

## Reflections:

This was really a tough assignment. I reviewed the assignment early on and knew what the expectations were going forward in completing this assignment. I did not see the importance of this from members on this team.

When an assignment is due, I stressed several times that you cannot wait until the day of the assignment is due or midnight hour in working on this assignment. This assignment was due on the 25th and we had two weeks to work on this assignment. When I reviewed the taskers which still needed to be accomplished, I took the time out of my busy schedule to complete those tasks while others on the team did not. There were several moving parts to this assignment and not just the misuse case.

For this assignment, I felt we did not work as a team. Going forward, this team will need to commit more time in completing our homework assignments I realize that we are all busy, but one person should not be doing all of the work to get the team to the finish line.

Also going forward, I am expecting everyone on this team to do their part in completing our homework assignment on time. I also expect everyone on the team to do their fair share of work. This is not a one person team, but we have five talented members on the team.

In the next assignment, members of the team will need to start working on the assignment before the due date and not turn in the assignment the day of.

When you wait until the last day to turn in the assignment, you are putting our assignment at risk. Let’s do our part by submitting the required assignment on time to include not waiting until the last minute to do so. If I can commit the time to complete our assignment, so should others members on the team. I want to enjoy my weekends and evenings as well and not be stressed out in meeting our assignment deadline.

## References:

“7 Encryption Methods to Shield Sensitive Data from Prying Eyes.” *GetApp*, https://www.getapp.com/resources/common-encryption-methods/. Accessed 22 Sept. 2023.

*Acts & Regulations*. https://www.aba.com/banking-topics/compliance/acts. Accessed 22 Sept. 2023.

*CVE-2023-23942 | SUSE*. https://www.suse.com/security/cve/CVE-2023-23942.html. Accessed 22 Sept. 2023.

“Cybersecurity Framework Crosswalk.” *NIST*, Jan. 2020. *www.nist.gov*, https://www.nist.gov/privacy-framework/resource-repository/browse/crosswalks/cybersecurity-framework-crosswalk.

Initiative, Joint Task Force Transformation. *Managing Information Security Risk: Organization, Mission, and Information System View*. NIST Special Publication (SP) 800-39, National Institute of Standards and Technology, 1 Mar. 2011. *csrc.nist.gov*, https://doi.org/10.6028/NIST.SP.800-39.

“Nextcloud Security and Authentication White Paper.” *Security and Authentication*, Nextcloud, https://nextcloud.com/media/wp135098u/Security-Whitepaper-WebVersion-072018.pdf.

“Registrars.” *Register. BANK*, https://www.register.bank/registrars/. Accessed 22 Sept. 2023.

“Security and Privacy Controls for Information Systems and Organizations.” *Security and Privacy Controls for Information Systems and Organizations*, National Institute of Standards Technology, 8 July 2023, https://crsc.nis.gov/pubs/sp/800/53/r5/upd1/final.

“Missing Occ Folder.” *Nextcloud Community*, 27 June 2023, <https://help.nextcloud.com/t/missing-occ-folder/165048>.

*Apache Log4j Vulnerability Guidance | CISA*. 8 Apr. 2022, <https://www.cisa.gov/news-events/news/apache-log4j-vulnerability-guidance>.

*Nextcloud : Security Vulnerabilities, CVEs*. https://www.cvedetails.com/vulnerability-list/vendor\_id-15913/Nextcloud.html?page=1&order=1&trc=272&sha=2d0cfbc94543ad39ce394ff454065b62178643a9. Accessed 22 Sept. 2023.

*Nextcloud : Products and Vulnerabilities*. https://www.cvedetails.com/vendor/15913/Nextcloud.html. Accessed 22 Sept. 2023