IT SECURITY STUDY

CloudDrain

Results of a global
IT security study on the
security vulnerability

**« ownCloud / Nextcloud
Unprotected Data Directory »**

Sascha Brendel · Anna Brendel

LEDNERB

Index

Foreword

In our ever-changing digital world, the security of IT systems must be a key concern for organizations of all sizes and industries.

Our comprehensive study sheds light on a critical security vulnerability in ownCloud and Nextcloud instances and provides deep insights into the risks and challenges organizations face. We have observed that many organizations, from small businesses to large institutions, are inadequately prepared to deal with cybersecurity threats. Our Responsible Disclosure process clearly showed that communication between security researchers and organizations is often hampered by shortcomings in communication channels.

To close this gap, we recommend the implementation of a security.txt file, whereby our services offer a customized solution to maximize security. We hope that our findings and recommendations will help to make the digital landscape more secure.

LEDNERB

Lednerb IT-Security - Your partner for IT security

Our aim is to protect our customers' infrastructure as effectively and efficiently as possible against cyber threats of all kinds. We see our customers as partners and strive for long-term cooperation based on trust.

With over a decade of experience in web and IT security, we specialize in meeting the specific requirements of our customers.

Our goal is a sustainable, effective and long-term cooperation. We offer individual, targeted solutions that are suitable for both large and small companies.

OUR SERVICES

Managed vulnerability scan

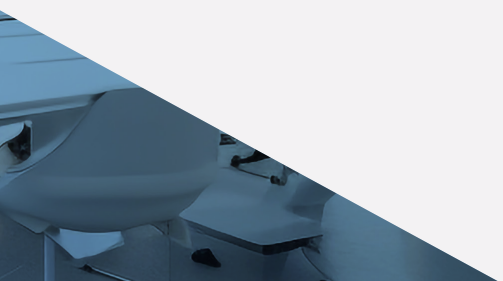
A vulnerability scan is an essential IT security measure for checking the security level of systems and applications. During a vulnerability scan, these are automatically checked by a vulnerability scanner for publicly known security vulnerabilities. Due to the daily increasing number of security vulnerabilities, the number of tests that are carried out during a scan is also rising. The scanner output is evaluated by IT security analysts and classified according to the respective risk.

Penetration test (external / internal)

A penetration test, also known as a pentest for short, is an IT security measure with the aim of checking the security level of systems and applications. A pentest is used to identify and evaluate both obvious and hidden vulnerabilities. The results are summarized together with corresponding recommendations for action in the form of a report.

IT security consulting

We value individual, targeted and comprehensive advice and offer you our expertise in IT security and data protection. We are happy to answer your questions and advise you on the following topics, among others: Backing up and restoring data, developing security strategies, creating threat analyses, procedures for reporting vulnerabilities, minimizing dependencies on third-party providers, encrypting files and emails, etc.



Brief overview

Cloud computing and **cloud collaboration** are no longer just trends, but firmly established technologies that support companies of all sizes with digitalization. Cloud services offer a wide range of opportunities to increase efficiency, particularly in the area of online collaboration.

Self-hosted alternatives: ownCloud and Nextcloud

In addition to the big players in the cloud market such as Microsoft and Google, there are open source alternatives such as ownCloud and Nextcloud. These offer companies the opportunity to retain control over their data while benefiting from the advantages of the cloud.

Security vulnerabilities in cloud services: a serious risk

However, these systems are not free of risks. The « ownCloud / Nextcloud Unprotected Data Directory » vulnerability, which has been known since 2016 at the latest, poses a significant risk. The vulnerability usually occurs due to a misconfiguration of the web server and allows unauthorized, free access to all data of all users.

ownCloud / Nextcloud Unprotected data directory

If the web server is configured incorrectly, it is possible to access log files via a simple web request such as
`http://cloud.example.org/data/nextcloud.log` or
`http://cloud.example.org/data/owncloud.log`.

Sensitive user information can then be extracted from these files. This then enables access to all data stored by the user.

A simple call in the web browser according to the following pattern is sufficient for this:
`http://cloud.example.org/data/EXAMPLE_USER`

Study objective and methodology

The aim of this study is to investigate the extent of the security vulnerability « ownCloud / Nextcloud Unprotected Data Directory ».

A total of 921,220,480 domains were analyzed. Of these, over 255 million domains from European countries and over 655 million domains from the .com domain area were scanned.

To collect the data, a specially developed, high-performance scanner was used, which is specifically designed for this security vulnerability.

The scanner was published by us as an open source project.

Responsible Disclosure Procedure

An important component of this study is compliance with the Responsible Disclosure Procedure.

After identifying vulnerable systems, attempts were made to contact the affected companies and institutions to inform them about the vulnerability and the associated risks.

This approach not only serves to protect the affected systems, but also to promote the responsible handling of security vulnerabilities.

What exactly is responsible disclosure?

*Responsible disclosure is a key term in the world of **IT security**. It is a procedure in which security **vulnerabilities** are reported and fixed confidentially before they become public knowledge. This approach is based on three pillars: **confidentiality**, **collaboration** and a set **timeframe**.*

*The main objectives of responsible disclosure are to **protect users** and **prevent misuse** by cybercriminals. One of the biggest challenges is to balance the interests of researchers, companies and the public and to set a reasonable timeframe to fix the security vulnerability.*

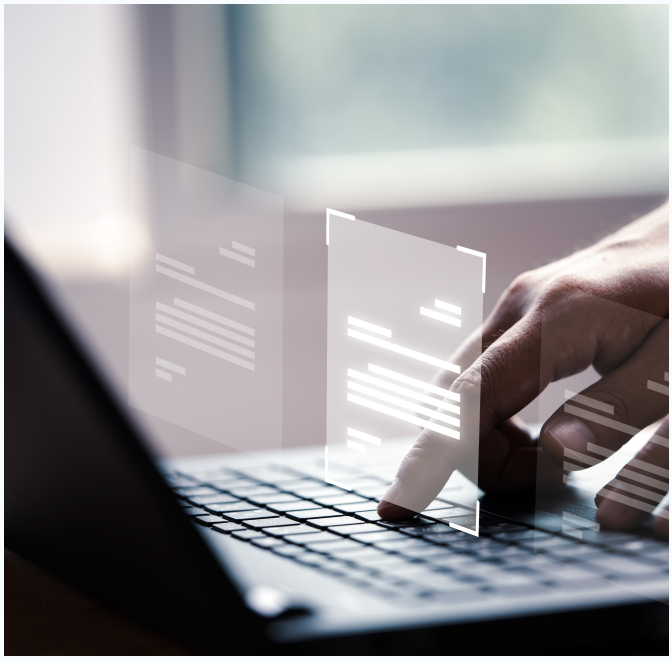
*The typical process of Responsible Disclosure includes the **discovery of the vulnerability**, the **confidential report** to the affected company, the **joint resolution of the problem** and finally the **publication** of the information after the issue has been resolved. This process plays a critical role in maintaining cybersecurity and protecting digital infrastructure.*


Cloud services
& online collaboration

What is online collaboration?

Online collaboration refers to the ability to work together on projects, documents or other tasks via the internet. This type of collaboration enables teams to communicate in real time and work together on projects, regardless of their geographical location. The tools used for this often include functions such as document sharing, video and audio conferencing, project management and more.

Support for the digitalization of companies



These online collaboration tools play a crucial role in the digitalization of companies. By providing platforms for efficient communication and collaboration, they facilitate the transition from traditional working methods to modern, digitalized processes. They not only enable the automation of manual tasks, but also promote teamwork and increase productivity. This is particularly invaluable in the current era of remote working.

Established providers on the market

There are a large number of providers that offer tools for online collaboration.
Some of the well-known solutions are:

Microsoft Teams

Video conferencing, file sharing and integration with other Microsoft products

Slack

Chat, audio communication and integrations with other services

Google Workspace

E-mail, calendar, video conferencing and various office tools

Zoom

Video conferencing, screen sharing functions and other forms of collaboration

Atlassian

Project management, ticket system, code and knowledge management

Data protection & data sovereignty

While online collaboration tools offer numerous benefits in terms of efficiency and productivity, they also raise important issues in terms of data protection and data sovereignty. Many of the major providers, such as Microsoft and Google, are US companies and are therefore subject to US legislation, which in some aspects has less stringent data protection regulations than the European Union. This can be particularly problematic when it comes to the storage of sensitive or personal data.

ownCloud & Nextcloud as self-hosted/managed alternatives

ownCloud and Nextcloud are two prominent open source solutions for file sync and online collaboration. In contrast to cloud services from US providers, ownCloud and Nextcloud can be hosted on own servers or in a trusted data center. This gives companies and organizations greater control over their data and strengthens data sovereignty.

Managed instances

Some providers offer "managed" ownCloud or Nextcloud instances. In this case, the service provider takes over the installation, maintenance and updating of the software, while the company can concentrate on its core competencies. These services can be hosted either in the company's own data center or by an external service provider.

Self-hosted instances

With a self-hosted instance, the full responsibility for installation, maintenance and security lies with the company itself. Although this requires more expertise, it offers maximum control over the data and infrastructure.

Advantages over US providers

- **Data sovereignty:** Since the data is stored in your own data center or with a trustworthy local provider, dependence on foreign legal systems is minimized.
- **Data protection:** By controlling your own servers, you can implement stricter data protection guidelines and technologies that comply with EU law.
- **Customizability:** As open source solutions, ownCloud and Nextcloud offer the option of adapting the software to specific needs and require-ments.
- **Costs:** Compared to license-based solutions, open source alternatives can be more cost-efficient in the long term, especially if they are self-managed.

« ownCloud / Nextcloud Unprotected Data Directory »

Course of the attack

Step 1

Download the log file

The log file may already contain sensitive information including user, directory and file names.

Step 2

Extraction of user names

The captured usernames can also be used for further attacks and phishing campaigns.

Step 3

Access to the directory

By simply calling up a URL in the web browser, an attacker gains full access to all stored data.

Due to a misconfiguration of the web server, an attacker can, in extreme cases, access all files stored in the respective cloud. The attacker does not need to know any login details or use complicated hacking procedures to do this.

Vulnerability description

The vulnerability « ownCloud / Nextcloud Unprotected Data Directory » results from a misconfiguration of the web server. This allows unprotected access to sensitive log files and possibly also user data.
The effects may vary depending on the extent of the misconfiguration:

- **Access to log files:** In this case, sensitive and personal data is potentially at risk. User names can be extracted from the log files.

- **Critical misconfiguration:** In the event of a particularly serious misconfiguration, access to individual user directories is possible. An unauthorized and unauthenticated attacker can then access all stored data, different file versions and even "deleted" files that are still in the recycle bin.

Causes for the existence of the vulnerability

The main causes for the existence of this vulnerability are usually insufficient knowledge of the web server configuration or neglected security policies.
It is important to emphasize that all established vulnerability scanners can detect this specific vulnerability for free, which makes the neglect of regular vulnerability scanning even more serious.

Checking the vulnerability

The existence of the vulnerability can be easily checked by calling the URL of the data directory (*/data/*) in the web browser.
If access to the files is gained, the instance is vulnerable.

For example, the following URL can be used for a Nextcloud instance:

http://cloud.example.org/data/nextcloud.log

For an ownCloud instance, the URL would be accordingly:

http://cloud.example.org/data/owncloud.log

Recommendation for action

If a vulnerable instance is detected, the web server configuration should be checked and adjusted as quickly as possible so that unauthenticated access to sensitive data and directories is blocked. After securing the system, it should be checked for signs of unauthorized access.

Results of the IT security study

This study illustrates the extent of vulnerable ownCloud and Nextcloud instances with regard to the vulnerability investigated.
The results are alarming and raise important questions about IT security and the responsible handling of regular security checks of external company infrastructures.

921
million

With a specially developed, high-performance vulnerability scanner, a total of over 921 million domains were examined.

Not only domains from European countries were scanned, but also over 655 million domains of the .com top level domain.

655
million

9624
Instances

9264 vulnerable instances were identified, affecting a wide range of industries.
As a result, cybercriminals not only have full access to highly sensitive data of the affected organizations, but also to the sensitive personal data of the respective customers stored therein.

Lednerb / CloudPeeker

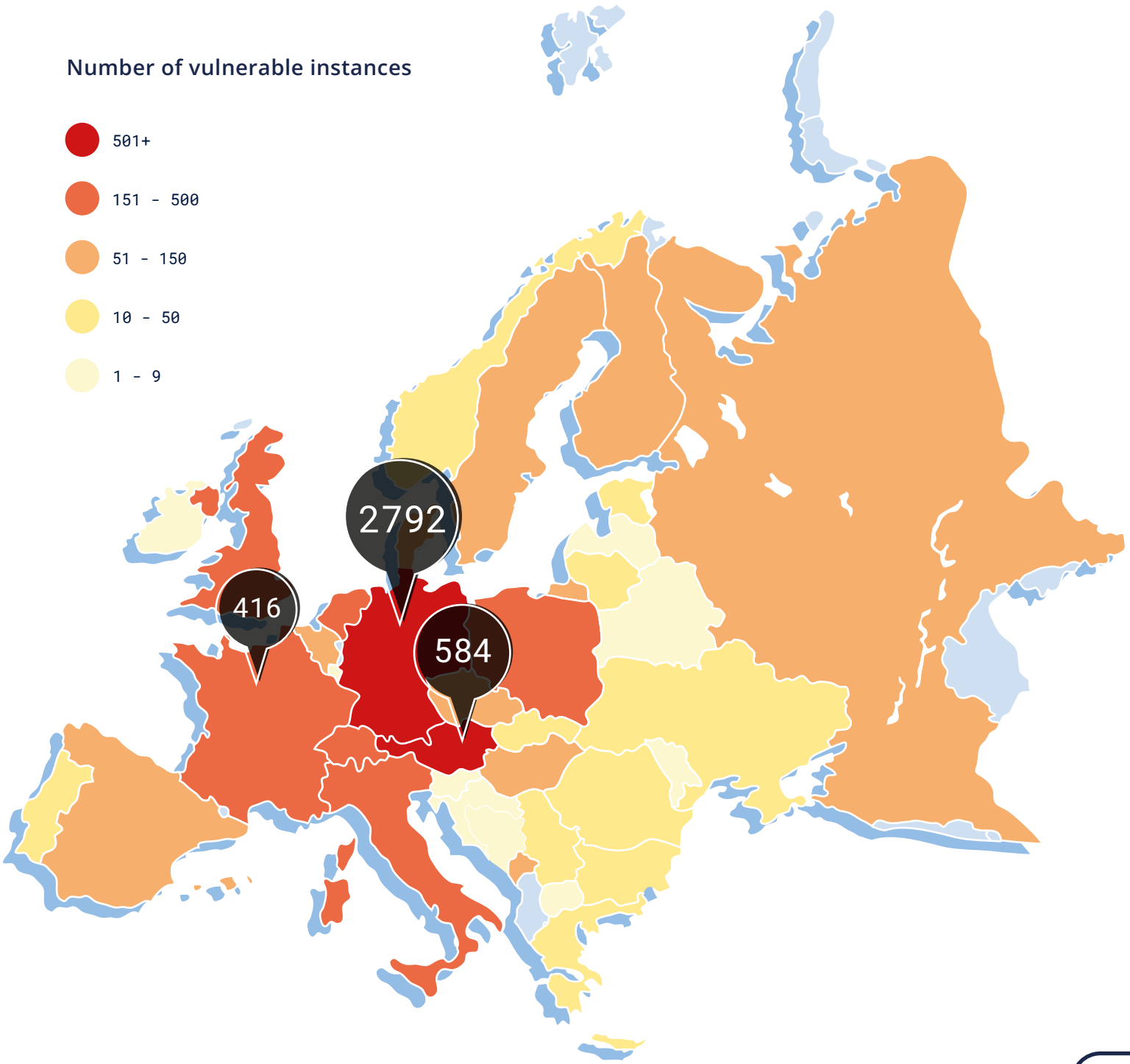
Our specially developed, high-performance scanner for the security vulnerability « owncloud / Nextcloud Unprotected Data Directory » was published under an open source license:

https://github.com/Lednerb/CloudPeeker

Spread of the vulnerability in Europe

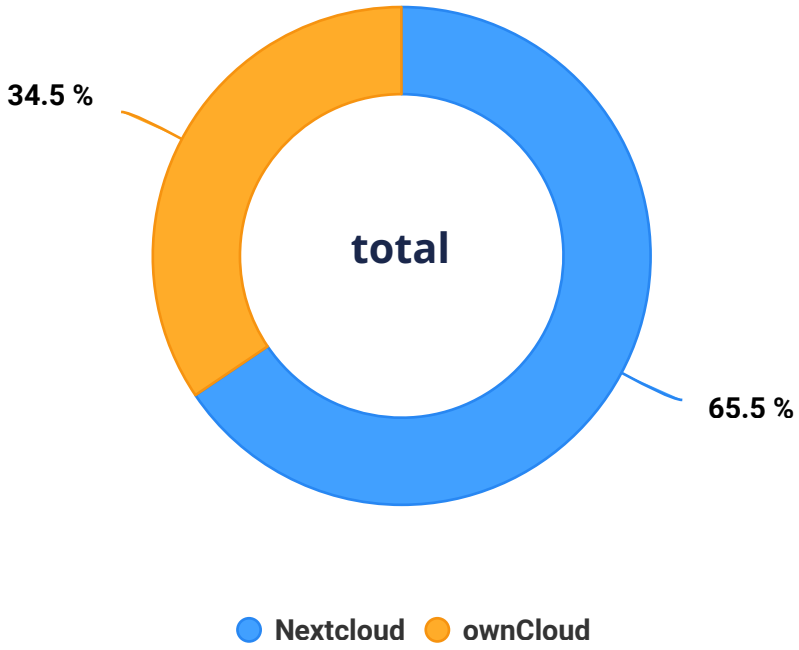
A total of 6954 affected instances of ownCloud and Nextcloud were identified among the European top-level domains, with over 50% of these cases - namely 3595 instances - being located in the DACH region. The distribution of these instances in Europe shows a clear concentration in certain countries. The top 3 countries with the most affected instances are Germany, Austria and France.

6954
Instances



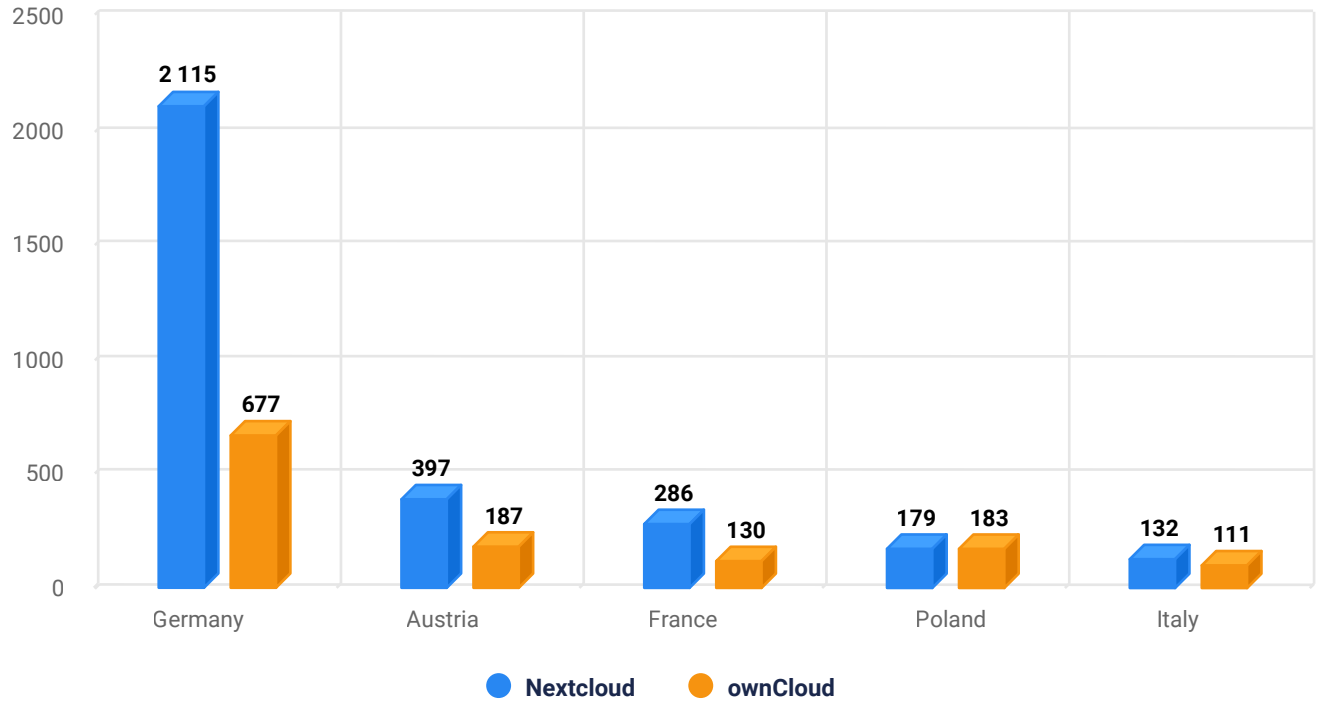
Distribution of vulnerable ownCloud / Nextcloud instances

Globally, the distribution of vulnerable instances shows a clear preponderance of Nextcloud, which accounts for 65.5% of affected installations, compared to 34.5% for ownCloud. This distribution is also reflected in the analysis of specific countries, with significant differences in the use of the two cloud services.
The European TLD (.eu) recorded 579 vulnerable instances with a distribution of 383 Nextcloud to 200 ownCloud instances.



When comparing the five countries Germany, Austria, France, Poland and Italy, it is noticeable that in the data sets of vulnerable instances Nextcloud occurs more frequently overall than ownCloud. In Germany and Austria, where the most vulnerable instances were identified, the proportion of Nextcloud instances is significantly higher than that of ownCloud. In France, Poland and Italy, this trend is also evident, but with a smaller difference between the two applications.

Splitting of vulnerable ownCloud & Nextcloud instances



Affected industries & companies

Among the 9624 vulnerable instances detected are numerous private users, but also a significant proportion of companies and organizations of various sizes and industries.

The affected institutions include law firms, hospitals, physicians' practices, power producers and IT service providers. Public administrations, such as cities and municipalities, and various non-profit organizations are also among those affected. The vulnerability also affected data protection officers, whose main responsibility is to protect sensitive customer data.

In the private sector, this vulnerability enables unprotected access to personal information such as family photos, financial data, personal documents and Bitcoin wallets. For companies, there is a high risk that sensitive information about customers or suppliers, patient data or access to servers will be unprotected and accessible to attackers.

This wide range of affected data and industries demonstrates the urgent need to strengthen cybersecurity measures across a broad spectrum of use cases.

In addition, educational institutions and universities were also affected by this vulnerability, allowing potential access to research data, student information and internal documents.

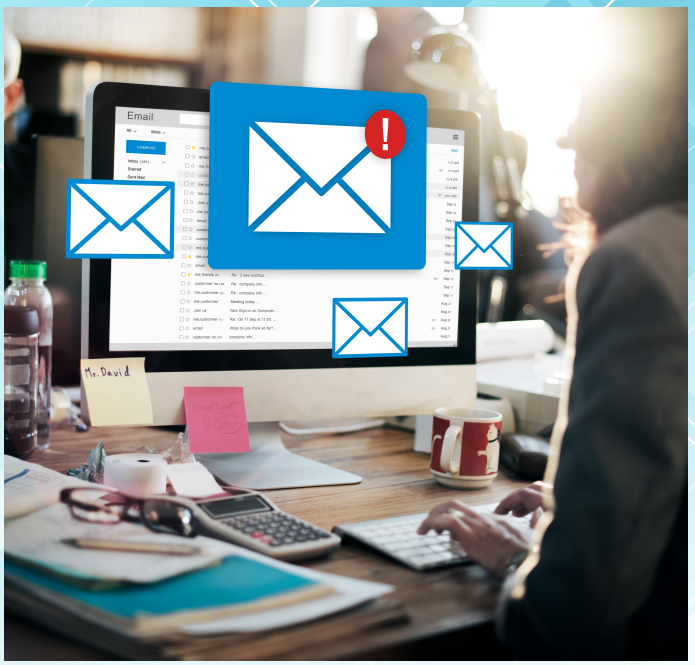
This raises serious concerns about the protection of intellectual property and sensitive research data. Also affected were small and medium-sized companies, which often do not have the resources or expertise to adequately protect their systems.

This makes them a particularly vulnerable target for cyberattacks.

At the time of publication of our study, it was determined that the official Nextcloud Security Scan (`https://scan.nextcloud.com`) did not detect the vulnerability highlighted here, although it is relatively easy to check.
The fact that an essential tool used by Nextcloud users to scan their systems does not detect this specific vulnerability underlines the need for more comprehensive and regular security checks.

Findings from our responsible disclosure process

As part of our responsible disclosure process, we have focused on contacting affected companies to inform them about the critical vulnerability in their ownCloud and Nextcloud instances. This approach was chosen because contacting private individuals often failed due to a lack of contact information and the impact of data theft on companies, especially in sensitive industries such as healthcare or lawyers, IT service providers and data protection officers, is more serious than for private individuals.



Our first step in establishing contact was to try to reach the respective data protection officers of the companies by email. We were astonished to find that around 70% of the privacy@ e-mail addresses did not work, as the accounts were either full or simply did not exist. In cases where no specific data protection officer details were available, we used general company email addresses. Our emails were mostly classified as spam or overlooked in the flood of messages, resulting in only about 3-5% of the companies and institutions contacted responding. This became clear when we contacted them again at a later time.

When trying to reach the right contact person by phone, we often encountered challenges. In many cases, we were not forwarded to the responsible person and were often verbally attacked and insulted. Nevertheless, there was also positive feedback from some managing directors and IT administrators who took the vulnerability seriously and initiated appropriate security measures. However, this process was costly and time-consuming.

In a further experiment, we sent a detailed security report by post to the 100 largest affected companies and institutions.

This contained a cover letter, the security report with a description of the vulnerability and screenshots of the exposed data, as well as recommendations for action to secure the instances. We also offered a log file analysis to determine whether the vulnerability had already been actively exploited.
However, we received no response to these mailings. After two months, a further check showed that 53 of the companies contacted had fixed the security vulnerability.

These specific experiences illustrate and confirm the difficulties that white hat hackers and IT security researchers face when trying to make the Internet more secure. Their efforts to uncover and report critical vulnerabilities are often met with obstacles as their communications are drowned in a sea of spam messages and unsolicited sales pitches.

Organizations that regularly encounter unverified vulnerabilities often find it challenging to distinguish legitimate security alerts from misleading or fraudulent communications. These obstacles result in an inadequate response to valid security alerts, underscoring the importance of established and effective vulnerability management and cybersecurity threat communication processes in the corporate world.

It is therefore crucial to increase cybersecurity awareness and promote the implementation of proactive security strategies in all types of organizations to ensure a robust and resilient digital infrastructure.

Provision of a communication channel within your own company

An effective way to benefit from the global cybersecurity community and strengthen the security of your own IT infrastructure is to implement a `security.txt` file.

This simple but effective standard provides a clearly defined way for security researchers and white hat hackers to confidentially report potential vulnerabilities. Information on how to implement this standard can be found at `https://securitytxt.org`

While the establishment of such a file is an important step, it also brings challenges. An increased volume of spam messages and the risk of receiving fraudulent or malicious "IT security reports" are real. To address these challenges and ensure that incoming reports are carefully checked and processed, we at Lednerb IT-Security GmbH offer a specialized service. This aims to maximize the benefits of a `security.txt` file while minimizing the risks.

Our service:

External
IT security contact

- ✔ Provision
- ✔ Filtering
- ✔ Analysis
- ✔ Verification
- ✔ Report creation

LEDNERB

Further information about our services can be found on our website:

`https://lednerb.de/en/external-security-contact`

Lednerb IT-Security GmbH

+49 461 99 58 3448

https://lednerb.de

Lise-Meitner-Straße 2
24941 Flensburg
Germany

LEDNERB