I. Introduction

CVE-2024-0204 is an authentication bypass vulnerability in Fortra's GoAnywhere MFT (Managed File Transfer) product. This vulnerability allows an unauthenticated attacker to create an administrative user for the application. The vulnerability is remotely exploitable and is listed as CWE-425: Forced Browsing, a weakness that occurs when a web application does not adequately enforce authorization on scripts or files.

The vulnerability affects Fortra GoAnywhere MFT versions 6.x from 6.0.1 and versions 7.x before 7.4.1. It was fixed in version 7.4.1, which was released on December 7, 2023. In terms of threat landscape, in 2023, file transfer applications were a top target by threat actors, highlighting the importance of securing such applications.

The vulnerability was originally discovered by researchers malcolm0x and Islam Elrfai. Fortra made customers aware of the issue through an internal security advisory post and made a patch available on December 4, 2023. Also, a proof-of-concept (PoC) exploit code for this vulnerability has been made public.

The advisory suggests that the vulnerability can be mitigated by deleting the endpoint /InitialAccountSetup.xhtml and restarting the service. For container-deployed instances, the file can be replaced with an empty file and then the service can be restarted.

II. GoAnywhere Managed File Transfer (MFT)

GoAnywhere Managed File Transfer (MFT) is a secure software solution that streamlines the exchange of data between systems, employees, customers, and trading partners. It is designed to centralize, simplify, and automate data movements, improving security and meeting compliance requirements.

GoAnywhere MFT can be deployed in various environments including on-premises, in the cloud on platforms like Microsoft Azure and AWS, or within hybrid environments. It is compatible with multiple operating systems such as Windows, Linux, AIX, and IBM i.

The software provides an intuitive browser-based interface with drag-and-drop controls, allowing users to easily customize their dashboard. It also offers a comprehensive set of workflow features that help eliminate the need for single-function tools, manual processes, or unsecure file transfer methods like FTP servers.

GoAnywhere MFT supports a wide range of protocols for secure file transfer, including SFTP (FTP over SSH), FTPS (FTP over SSL/TLS), SCP (Secure Copy over SSH), HTTP/s, AS2, AS3, AS4, and others. It also provides over 60 different tasks that can be chained together in workflows, with no programming or scripting required.

In addition to its core file transfer capabilities, GoAnywhere MFT also includes features for password security, two-factor authentication, and integration with various other systems and applications.

III. Industries covered by GoAnywhere Managed File Transfer (MFT)

GoAnywhere Managed File Transfer (MFT) is commonly used across a variety of industries due to its ability to securely automate the exchange of data. The top industries that use GoAnywhere MFT include:

- Information Technology and Services
- Computer Software
- Financial Services
- Hospital & Healthcare
- Manufacturing
- Consulting

In the IT and services industry, GoAnywhere MFT is used to integrate with web and cloud applications, ensuring data security and providing secured and automated file transfers using a centralized enterprise-level approach. It can also be used to standardize file transfer processes, reducing the need to involve development teams when transferring files:

- **Integrating with Web and Cloud Applications**: It helps in securely integrating file transfers with web and cloud-based applications.
- **Centralizing File Transfer Processes**: GoAnywhere MFT provides a centralized platform to manage all file transfers, reducing the need for development teams to be involved in the transfer process.
- **Automating File Transfers**: It automates repetitive and complex file transfer tasks, saving time and reducing errors.
- **Enhancing Security**: The solution offers enterprise-level security features, helping IT services firms to protect sensitive data during transfers.

In the computer software industry, GoAnywhere MFT can be used to automate and secure file transfers, reducing the need for custom scripts and manual processes. It can also be used to create, edit, and monitor file transfer jobs, and to perform various workflows and data translations.

- **Automating Software Distribution**: Securely automating the distribution of software updates and patches to clients.
- **Collaboration**: Enabling secure collaboration between developers, especially when working with source code and other sensitive data.
- **Regulatory Compliance**: Assisting software companies in meeting compliance requirements for software development and data handling.

In the financial services industry, GoAnywhere MFT is used to protect sensitive customer data and meet compliance requirements. It helps control the exchange of sensitive cardholder data and track file movements for easy auditing. For example, Sentinel Benefits & Financial Group uses GoAnywhere MFT to create and edit file transfer jobs, monitor security, perform various workflows, and complete hundreds of transactions in seconds.

- **Secure Transactions**: Automating and securing financial transactions, ensuring sensitive data is protected.
- **Compliance**: Meeting strict compliance requirements such as PCI DSS for the protection of cardholder data.
- **Efficient Data Handling**: Streamlining the process of creating, editing, and monitoring file transfer jobs, as demonstrated by Sentinel Benefits & Financial Group.

In the healthcare industry, GoAnywhere MFT can be used to securely transfer patient data and other sensitive information, helping healthcare organizations meet compliance requirements such as HIPAA. It can also be used to automate file transfers, reducing the need for manual processes and improving efficiency.

- **Patient Data Protection**: Securely transferring patient health information (PHI) while complying with HIPAA regulations.
- **Secure Patient Data Exchange**: Securely exchanging patient data between healthcare providers, insurers, and other stakeholders.
- **Interoperability**: Facilitating the exchange of healthcare data between different systems and organizations.
- **Compliance with Healthcare Regulations**: Ensuring that data transfers comply with healthcare regulations such as HIPAA.
- **Automating Healthcare Data Transfers**: Automating the transfer of electronic health records (EHRs), lab results, and other critical healthcare data.
- **Automating Healthcare Workflows**: Automating the transfer of lab results, billing information, and other healthcare-related data.

In the manufacturing industry, GoAnywhere MFT can be used to automate and secure the transfer of design files, production data, and other sensitive information. It can also be used to integrate with other systems and applications, improving efficiency and reducing the need for manual processes.

- **Secure Design File Transfers**: Protecting the transfer of sensitive design and production files.
- **Supply Chain Integration**: Integrating with supply chain partners for efficient data exchange.
- **Automating Manufacturing Processes**: Automating the transfer of manufacturing data, such as inventory levels, order data, and shipment tracking.

In the consulting industry, GoAnywhere MFT can be used to securely transfer sensitive client data and other information. It can also be used to automate file transfers, reducing the need for manual processes and improving efficiency.

- **Client Data Security**: Ensuring the secure transfer of sensitive client data during consulting engagements.
- **Project Collaboration**: Facilitating secure collaboration on projects that involve data sharing between consultants and clients.
- **Efficiency and Automation**: Automating the exchange of data and reports with clients, improving efficiency and reducing manual effort.

IV. Root Cause of CVE

The root cause of CVE-2024-0204 is identified as CWE-425: Forced Browsing. This weakness occurs when a web application does not adequately enforce authorization on scripts or files, allowing attackers to bypass authentication mechanisms and gain unauthorized access. Specifically, the vulnerability in Fortra's GoAnywhere MFT allows an unauthenticated attacker to create an admin user through the administration portal.

The exploit takes advantage of a path traversal issue, which is a type of security vulnerability that allows attackers to access files and directories that are stored outside the web root folder. Attackers can manipulate variables that reference files with dot-dot-slash (../) sequences and similar methods to access arbitrary files and directories stored on the file system. In the case of CVE-2024-0204, the path traversal issue allows access to the vulnerable /InitialAccountSetup.xhtml endpoint of the GoAnywhere MFT administration portal.

Once the attacker has access to this endpoint, they can create an administrative user with all the associated admin read and write permissions, and command execution capabilities. This effectively bypasses the normal authentication requirements, as the attacker does not need to provide any valid credentials to gain administrative access to the system.

This vulnerability is particularly risky for customers who have an admin portal exposed to the internet, as it makes the system easily accessible to potential attackers.

V. CVE Impact and Affected Systems

The impact of CVE-2024-0204 on GoAnywhere MFT users is significant due to the critical nature of the vulnerability. Here are the key impacts:

- **Creation of Unauthorized Admin Users**: The vulnerability allows an unauthenticated attacker to create an administrative user, which could lead to unauthorized access to the system
- **Potential for Data Breach**: With administrative access, attackers could potentially access sensitive data, which could result in a data breach
- **Malware Deployment**: Attackers with admin privileges could deploy malware, including ransomware, which could disrupt operations and lead to financial losses
- **Complete System Takeover**: The creation of admin-level users could allow attackers to take complete control of the affected system
- **Risk of Extortion**: Given the ease of exploitation, there is a risk of extortion, with attackers potentially threatening to publish sensitive data unless they receive payment
- **Operational Disruption**: Unauthorized access and potential subsequent attacks could disrupt the normal operations of the affected organizations
- **Compliance and Legal Issues**: Organizations affected by a breach resulting from this vulnerability could face compliance issues and legal consequences

GoAnywhere MFT has a CVSS score of 9.8 (severity of the vulnerability). It's also worth noting that a proof-of-concept exploit for this vulnerability has been made public, which could potentially make it easier for attackers to exploit this vulnerability.

The difference between a CVSS score of 9.8 and 10.0 primarily lies in the "Scope" metric within the CVSS scoring system. A CVSS score of 10.0 indicates that the vulnerability has the most severe impact and exploitability metrics, and its impact extends beyond the vulnerable component itself, affecting other components as well. In contrast, a CVSS score of 9.8 also represents a vulnerability with the most severe exploitability and impact metrics, but its impact does not extend beyond the vulnerable component.

In simpler terms, a CVSS score of 10.0 suggests a vulnerability that can cause more widespread damage across the system, potentially compromising additional systems beyond the initial point of exploitation. A score of 9.8, while still critical, indicates a vulnerability that is confined to the affected component and does not have the ability to impact other parts of the system.

VI. Attack Flow and Scenario

The attack complexity level of CVE-2024-0204 is low. This means that the conditions required to exploit the vulnerability are not difficult to achieve, and the attack can be carried out consistently without any special conditions. The low complexity level, combined with the critical severity of the vulnerability, makes it a significant security concern.

A. Attack flow

The attack flow for CVE-2024-0204, an authentication bypass vulnerability in Fortra's GoAnywhere MFT, is as follows:

- **Initial Access**: The attacker, who is unauthenticated, accesses the GoAnywhere MFT administration portal. This is possible due to the path traversal issue that the vulnerability presents
- **Exploitation**: The attacker exploits the path traversal issue to gain access to the /InitialAccountSetup.xhtml endpoint
- **Creation of Admin User**: Once the attacker has access to the /InitialAccountSetup.xhtml endpoint, they can create an administrative user. This user has all the associated admin read and write permissions, and command execution capabilities
- **Potential Further Exploitation**: With administrative access, the attacker could potentially access sensitive data, deploy malware, or take complete control of the system

B. Attack scenario

Potential attack scenarios for CVE-2024-0204 could include:

- **Ransomware Attacks**: Given the history of file transfer products being used as gateways for ransomware attacks, there is a concern that CVE-2024-0204 could be exploited in a similar manner. Attackers could use the admin access gained through this vulnerability to deploy ransomware, encrypting files and demanding a ransom for their decryption
- **Data Exfiltration**: Attackers could use the admin access to exfiltrate sensitive data. This could include personal data, financial information, or proprietary business data. The stolen data could be sold on the dark web, used for identity theft, or used to gain a competitive advantage
- **System Takeover**: With admin access, attackers could potentially take complete control of the system. This could be used to disrupt operations, deploy additional malware, or use the system as a launchpad for further attacks
- **Extortion**: Attackers could threaten to publish sensitive data unless they receive payment. This could be particularly damaging for organizations that handle sensitive customer data or proprietary information
- **Sabotage**: In a more destructive scenario, attackers could use the admin access to delete or alter data, disrupt operations, or otherwise sabotage the organization. This could result in significant business impacts, including downtime and financial losses

VII. Consequences

The potential consequences of an attack exploiting CVE-2024-0204 on GoAnywhere MFT users include:

- **Unauthorized Administrative Access**: Attackers can create an admin user via the administration portal without proper authorization, leading to unauthorized access to the system
- **Data Breach**: With admin access, attackers could potentially access, exfiltrate, or manipulate sensitive data, leading to a data breach
- **System Compromise**: Attackers could leverage the admin access to further compromise the system, potentially affecting the integrity, availability, and confidentiality of the system and data
- **Operational Disruption**: The unauthorized access could be used to disrupt operations, which could have significant business impacts, including downtime and financial losses
- **Extortion and Ransomware**: There is a risk of extortion, with attackers threatening to publish sensitive data unless they receive payment. The vulnerability could also be used as a gateway for ransomware attacks, as seen with previous vulnerabilities in file transfer products
- **Reputation Damage**: A successful attack could damage the reputation of the affected organization, leading to loss of customer trust and potential legal consequences
- **Compliance Violations**: Organizations could face regulatory fines and sanctions if the breach results in non-compliance with data protection laws and industry regulations

VIII. CVE PoC

The GitHub link https://github.com/horizon3ai/CVE-2024-0204/ leads to a Python script, which is a PoC-exploit for the vulnerability. This script, developed by Horizon3.ai, demonstrates how the authentication bypass vulnerability in GoAnywhere MFT can be exploited.

The script works by sending a POST request to the /InitialAccountSetup.xhtml endpoint of the GoAnywhere MFT application. The request includes parameters to create a new administrative user, effectively bypassing the authentication mechanism.

A. Scripts parameters

These parameters include information necessary to create a new user account, such as:

- **Username**: The desired username for the new administrative account.
- **Password**: The password for the new account, which must meet the complexity requirements of GoAnywhere MFT.
- **Email Address**: The email address associated with the new administrative account.
- **Full Name**: The full name of the individual associated with the new account.
- **Permissions**: The level of access or roles assigned to the new user, in this case, administrative privileges.

These parameters are sent in the body of the HTTP POST request as part of the request payload. The server processes these parameters and creates a new user account with the specified details.

After running the PoC-script for CVE-2024-0204, the expected response would be an indication that the script successfully created a new administrative user in the GoAnywhere MFT application. The specific details of the response would depend on the application's behavior upon user creation, but generally, you might expect:

- **HTTP Success Response**: A status code indicating success (e.g., HTTP 200 OK) from the web server, signifying that the POST request was successfully processed.
- **Confirmation Message**: A message or JSON response from the application confirming that the new administrative user has been created.
- **Error Messages**: Error messages that would indicate the request was unsuccessful.
- **Administrative Access**: The ability to log in with the newly created administrative user credentials, confirming that the user has been created with the expected permissions.

IX. Other vulnerabilities related to CVE

Other vulnerabilities that have been discovered in GoAnywhere MFT include:

- CVE-2021-46830
- CVE-2023-0669

CVE-2021-46830 is a path traversal issue that could potentially allow an external user who self-registers to access unintended areas of the application. It affects versions of GoAnywhere MFT prior to 6.8.3.

CVE-2023-0669 is a pre-authentication command injection that could be exploited by an arbitrary user. It was specifically a concern for customers with an admin portal accessible through the internet. Vulnerability involves deserializing untrusted data without proper validation, impacting confidentiality and integrity.

A. Attack flow [CVE-2021-46830] and scenario

Based on the nature of CVE-2021-46830 the attack flow for such a vulnerability involves the following steps:

- **Discovery**: The attacker discovers that the web application is vulnerable to path traversal due to inadequate input validation.

- **Exploitation**: The attacker crafts a request that includes directory traversal sequences (e.g., ../) to navigate from the web root to directories that should be inaccessible.
- **Access**: The crafted request allows the attacker to access or execute files that are outside of the intended web-accessible directories.
- **Impact**: Depending on the files or directories accessed, the attacker could potentially read sensitive information, execute unauthorized commands, or leverage the access to further compromise the system.

For CVE-2021-46830 specifically, the vulnerability allowed an external user who self-registers to access unintended areas of the GoAnywhere MFT application, which could potentially lead to unauthorized information disclosure or further attacks.

A potential attack scenario could look like this:

- **Initial Access**: An attacker identifies a GoAnywhere MFT application that is accessible over the network and allows self-registration of users.
- **Exploitation**: The attacker self-registers and then manipulates file paths in the application to access directories and files outside of the intended scope.
- **Information Disclosure**: The attacker reads files that they should not have access to, potentially gaining access to sensitive information.
- **Further Attacks**: Depending on the nature of the accessed data and the functionality of the application, the attacker could potentially use the information gained to carry out further attacks.

B. Attack flow [CVE-2023-0669] and scenario

Based on the nature of CVE-2021-46830 the attack flow for such a vulnerability involve the following steps:

- **Reconnaissance**: The attacker identifies a vulnerable target system that is accessible and has the specific vulnerability, in this case, CVE-2023-0669.
- **Crafting the Attack**: The attacker creates a malicious input or payload designed to exploit the vulnerability.
- **Delivery**: The attacker sends the crafted payload to the target system. This could be through network requests, malicious files, or other means depending on the nature of the vulnerability.
- **Exploitation**: The payload triggers the vulnerability, allowing the attacker to execute arbitrary code or commands, bypass security mechanisms, or otherwise compromise the system.
- **Post-Exploitation**: After successful exploitation, the attacker may perform actions such as establishing persistent access, escalating privileges, stealing data, or spreading to other systems.

A potential attack scenario for a vulnerability like CVE-2023-0669, which requires human interaction, could involve:

- **Social Engineering**: An attacker might use social engineering techniques to trick a user into performing certain actions that would trigger the vulnerability. This could involve sending a malicious document or link to the user.
- **Malicious Document**: The attacker could craft a document that exploits the vulnerability when opened or interacted with by the user. This document could be disguised as a legitimate file to increase the chances of the user opening it.
- **Remote Code Execution**: If the vulnerability allows for remote code execution, the attacker could potentially execute arbitrary code on the victim's system once the malicious document is processed.
- **Privilege Escalation**: The attacker could use the vulnerability to gain higher privileges on the system, potentially leading to a full system compromise.
- **Data Theft or Manipulation**: With the ability to execute code, the attacker could steal sensitive data, manipulate data, or install additional malicious software on the system.
- **Persistence**: The attacker could establish a persistent presence on the affected system, allowing for continued access and further exploitation.

C. Attack flow and scenario differences

In terms of impact, CVE-2024-0204 allows an attacker to bypass authentication and create an admin user, while CVE-2021-46830 allows an attacker to traverse directories and access or execute files outside of the intended web-accessible directories.

In terms of impact, CVE-2024-0204 involves a path traversal issue in a web application that allows an attacker to bypass authentication and create an admin user, while CVE-2023-0669 involves a vulnerability that can be triggered by processing a specially crafted document.

In terms of scenario, CVE-2024-0204 involves an attacker gaining full administrative access to the system, while CVE-2021-46830 involves an attacker gaining unauthorized access to certain areas of the application.

In terms of scenario, the key difference between the two is that CVE-2024-0204 allows for direct administrative access without the need for user interaction, while CVE-2023-0669 requires a user to interact with a malicious document to trigger the vulnerability. CVE-2024-0204 is a web application vulnerability, whereas CVE-2023-0669 involves document handling, likely in a desktop or server context.

D. Impact [CVE-2021-46830]

The impact of CVE-2021-46830 is that it allows an external user who self-registers to access unintended areas of the GoAnywhere MFT application. This could potentially lead to unauthorized information disclosure or further attacks.

The severity of the impact would depend on the specific data and functionality exposed by the unintended access. For example, if the accessed areas contain sensitive data, the attacker could potentially steal this data. If the accessed areas allow the execution of certain commands or functions, the attacker could potentially use this to further compromise the system.

E. Impact [CVE-2023-0669]

The impact of CVE-2023-0669 could include:

- **Unauthorized Access**: The attacker could potentially gain unauthorized access to the system or data, depending on the nature of the vulnerability and the system's configuration.
- **Data Theft**: If the vulnerability allows access to data, the attacker could potentially steal sensitive information.
- **System Compromise**: In some cases, the attacker could potentially use the vulnerability to execute arbitrary code or commands, which could lead to a full system compromise.
- **Denial of Service**: If the vulnerability causes the system to crash or become unresponsive, it could potentially lead to a denial of service.

F. Impact diffenences

CVE-2024-0204 has a more severe impact as it allows an attacker to gain full administrative access to the system, while CVE-2021-46830 could potentially lead to unauthorized information disclosure or further attacks.

CVE-2024-0204 has a more severe impact as it allows an attacker to gain full administrative access to the system, while the impact of CVE-2023-0669 would depend on the nature of the vulnerability and the system's configuration.

G. Consequences [CVE-2021-46830]

The potential consequences of an attack exploiting this vulnerability could include:

- **Unauthorized Access**: An attacker could potentially gain unauthorized access to directories and files outside of the intended scope. This could lead to unauthorized access to sensitive information or system resources.
- **Information Disclosure**: The attacker could potentially read files that they should not have access to, leading to the disclosure of sensitive information.
- **System Compromise**: Depending on the nature of the accessed data and the functionality of the application, the attacker could potentially use the information gained to carry out further attacks, potentially leading to a full system compromise.
- **Data Manipulation**: If the attacker gains write access to certain files or directories, they could potentially manipulate data, which could have various impacts depending on the nature of the data and the system's functionality.

H. Consequences [CVE-2023-0669]

The potential consequences of CVE-2023-0669 could include:

- **Unauthorized Access**: The attacker could gain unauthorized access to the system, potentially leading to further exploitation.
- **Data Theft**: The attacker could steal sensitive data from the compromised system, which could include personal, financial, or proprietary information.
- **System Compromise**: The attacker could execute arbitrary code, which could lead to a full system compromise, allowing them to modify, delete, or encrypt files.
- **Malware Deployment**: The attacker could use the vulnerability to deploy malware, including ransomware or a backdoor, to maintain persistent access to the system.
- **Denial of Service**: The attacker could disrupt services by crashing the system or consuming resources, leading to a denial of service.
- **Privilege Escalation**: If the vulnerability allows, the attacker could escalate their privileges on the system, gaining higher levels of control.

I. Consequences diffenences

CVE-2024-0204 could lead to a full system compromise due to unauthorized administrative access, while CVE-2021-46830 could lead to unauthorized access to certain areas of the application and potential information disclosure.

Both vulnerabilities could lead to a full system compromise, but they do so in different ways. CVE-2024-0204 involves unauthorized administrative access to a web application, while CVE-2023-0669 involves remote code execution, potentially through a path traversal flaw.