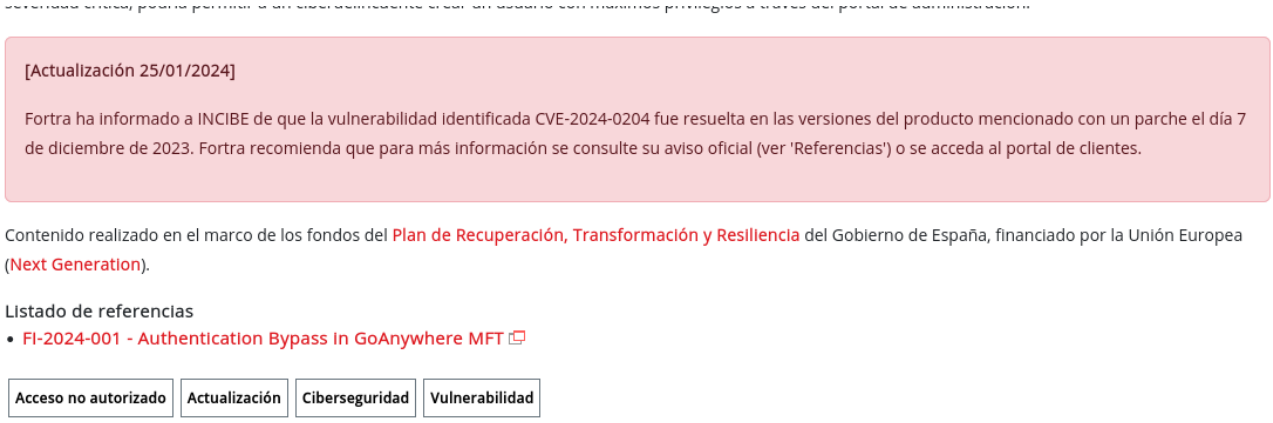
Trazado de Vulnerabilidad: GoAnywhere MFT de Fortra

Actualización de la Vulnerabilidad



[Actualización 25/01/2024]

Fortra ha informado a INCIBE de que la vulnerabilidad identificada CVE-2024-0204 fue resuelta en las versiones del producto mencionado con un parche el día 7 de diciembre de 2023. Fortra recomienda que para más información se consulte su aviso oficial (ver 'Referencias') o se acceda al portal de clientes.

Contenido realizado en el marco de los fondos del Plan de Recuperación, Transformación y Resiliencia del Gobierno de España, financiado por la Unión Europea (Next Generation).

Listado de referencias

- FI-2024-001 - Authentication Bypass in GoAnywhere MFT

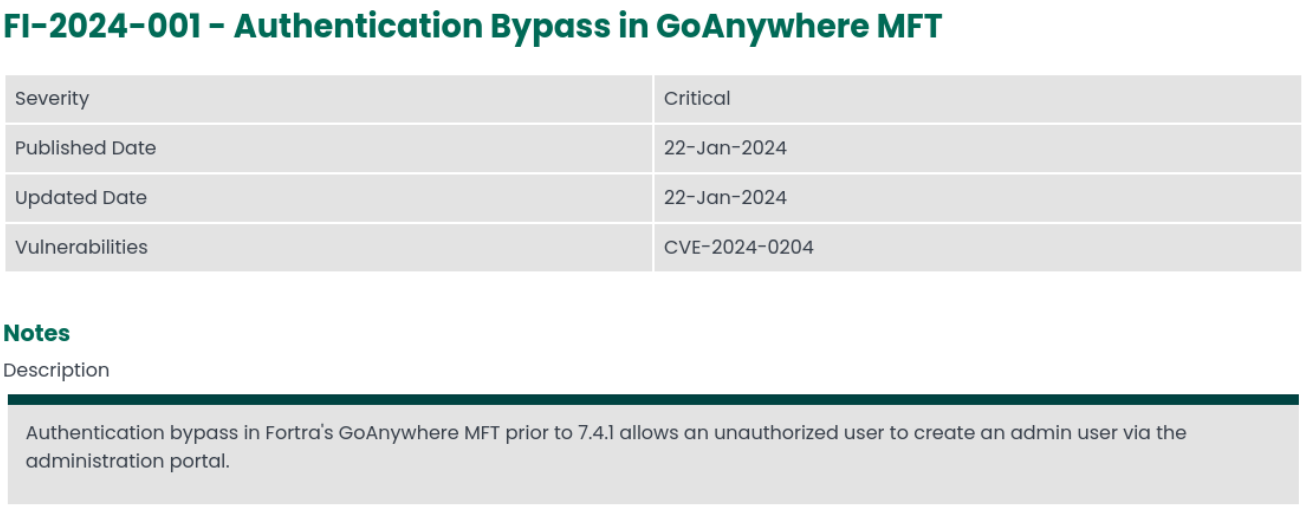
Acceso no autorizado | Actualización | Ciberseguridad | Vulnerabilidad

En esta primera captura vemos la actualización publicada el 25 de enero de 2024. Lo importante aquí es que **Fortra informó a INCIBE que la vulnerabilidad CVE-2024-0204 fue resuelta con un parche el 7 de diciembre de 2023**. Esto nos dice que es un problema serio que ya tiene solución disponible.

---

2. Información General de la Vulnerabilidad

Datos Básicos



FI-2024-001 - Authentication Bypass in GoAnywhere MFT

Severity	Critical
Published Date	22-Jan-2024
Updated Date	22-Jan-2024
Vulnerabilities	CVE-2024-0204

Notes

Description

Authentication bypass in Fortra's GoAnywhere MFT prior to 7.4.1 allows an unauthorized user to create an admin user via the administration portal.

En esta imagen se ve información de la Fortra sobre la vulnerabilidad. Podemos observar:

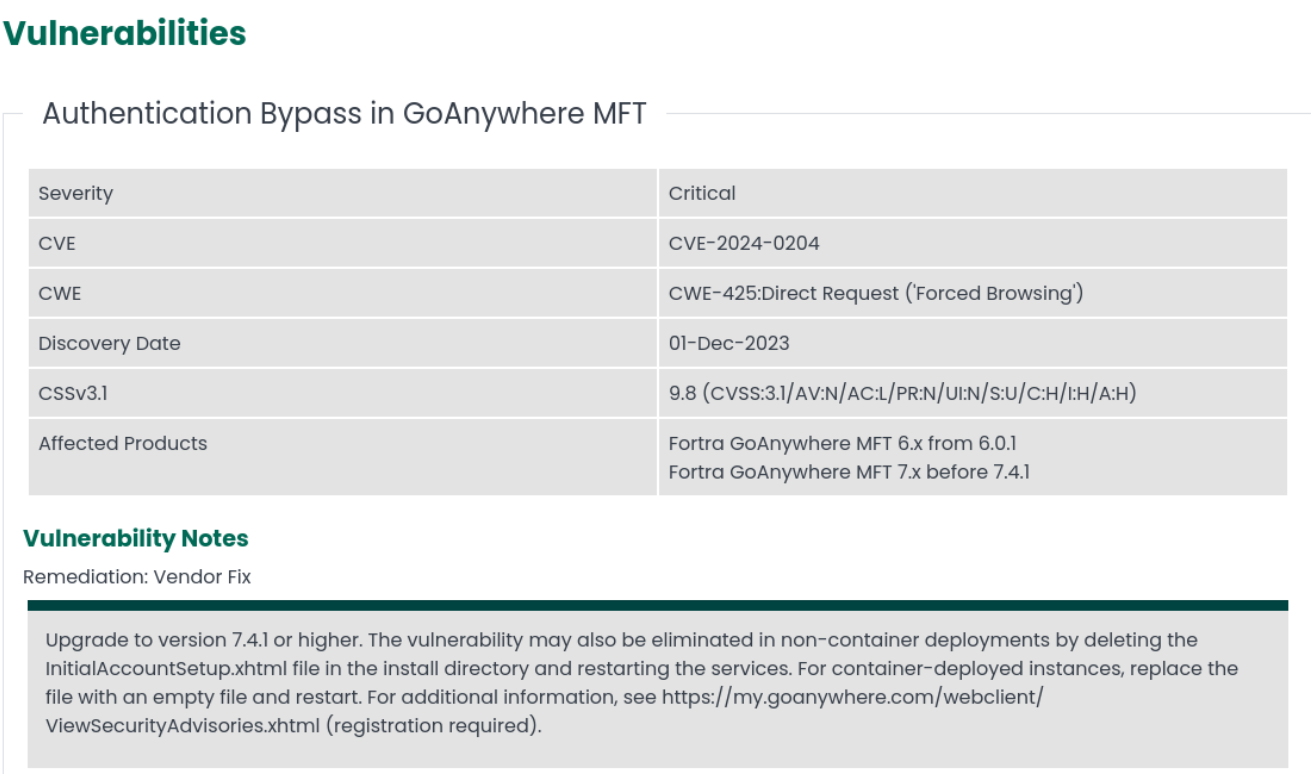
- **FI-2024-001**: Este es el identificador que Fortra le da a la vulnerabilidad
- **Severidad**: Crítica
- **Fecha de Publicación**: 22-Ene-2024
- **CVE**: CVE-2024-0204

También vemos que hay una referencia con etiquetas: **Acceso no autorizado**, **Actualización**, **Ciberseguridad** y **Vulnerabilidad**, lo que nos ayuda a clasificar este problema.

---

3. Descripción de la Vulnerabilidad

¿Qué es lo que falla?



Vulnerabilities

Authentication Bypass in GoAnywhere MFT

Severity	Critical
CVE	CVE-2024-0204
CWE	CWE-425:Direct Request ('Forced Browsing')
Discovery Date	01-Dec-2023
CSSv3.1	9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
Affected Products	Fortra GoAnywhere MFT 6.x from 6.0.1 Fortra GoAnywhere MFT 7.x before 7.4.1

Vulnerability Notes

Remediation: Vendor Fix

Upgrade to version 7.4.1 or higher. The vulnerability may also be eliminated in non-container deployments by deleting the InitialAccountSetup.xhtml file in the install directory and restarting the services. For container-deployed instances, replace the file with an empty file and restart. For additional information, see https://my.goanywhere.com/webclient/ViewSecurityAdvisories.xhtml (registration required).

En esta captura vemos la descripción del problema. Lo que entiendo es:

"La omisión de autenticación en GoAnywhere MFT de Fortra anterior a 7.4.1 permite a un usuario no autorizado crear un usuario administrador a través del portal de administración"

Esto significa que **alguien sin permiso podía entrar al panel de control y crear una cuenta de administrador sin necesidad de contraseña o credenciales válidas**. Es muy grave porque un administrador tiene control total del sistema.

En la tabla también vemos:

- Versiones afectadas desde **6.0.0 hasta 7.4.1**
- **Vector CVSS**: 9.8
- **Gravedad**: CRÍTICA

---

4. Información del CVE

Datos en la Base de Datos CVE

Descripción

La omisión de autenticación en GoAnywhere MFT de Fortra anterior a 7.4.1 permite a un usuario no autorizado crear un usuario administrador a través del portal de administración.

Impacto

Vector 3.x CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Puntuación base 3.x 9.80

Gravedad 3.x CRÍTICA

Productos y versiones vulnerables

CPE	Desde	Hasta
cpe:2.3:a:fortra:goanywhere_managed_file_transfer:*:*:*:*:*:*:*:*	7.0.0 *(incluyendo)*	7.4.1 *(excluyendo)*
cpe:2.3:a:fortra:goanywhere_managed_file_transfer:6.0.0:*:*:*:*:*:*:*		

Para consultar la lista completa de nombres de CPE con productos y versiones, ver esta página

Aquí vemos la información del CVE-2024-0204 en la base de datos oficial:

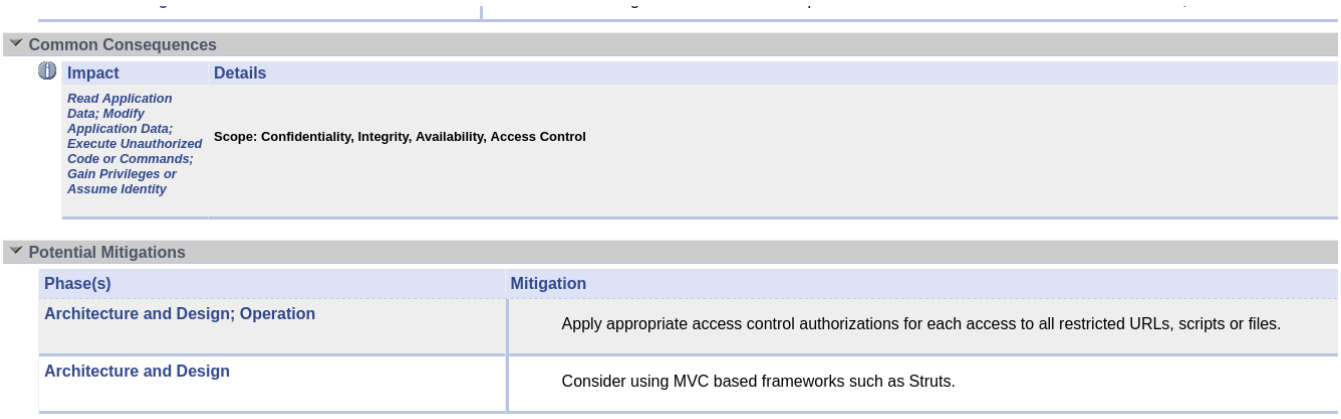
- **Severity**: Critical
- **Published Date**: 22-Jan-2024
- **Updated Date**: 22-Jan-2024
- **Vulnerabilities**: CVE-2024-0204

La información confirma que es crítica y fue publicada hace poco tiempo.

---

5. Debilidades Explotadas (CWE)

Primera Captura de Debilidades



Common Consequences

Impact	Details
Read Application Data; Modify Application Data; Execute Unauthorized Code or Commands; Gain Privileges or Assume Identity	**Scope: Confidentiality, Integrity, Availability, Access Control**

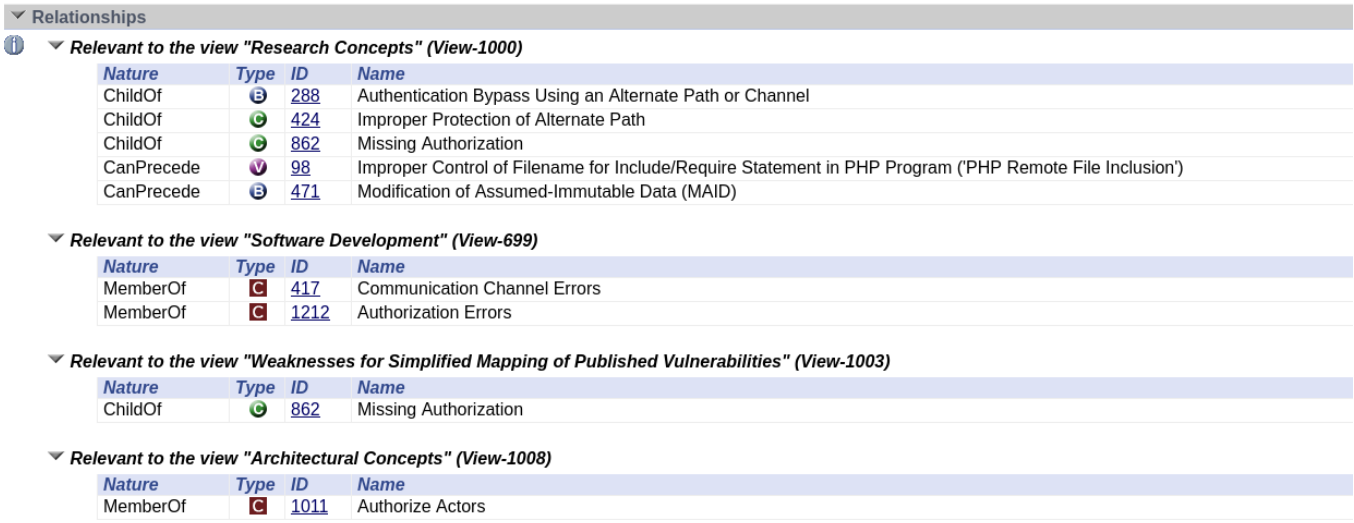
Potential Mitigations

Phase(s)	Mitigation
Architecture and Design; Operation	Apply appropriate access control authorizations for each access to all restricted URLs, scripts or files.
Architecture and Design	Consider using MVC based frameworks such as Struts.

Aquí vemos las relaciones de las debilidades:

- **CWE-288**: "Authentication Bypass Using an Alternate Path or Channel" - Esto es lo principal, que se puede saltarse la autenticación
- **CWE-424**: "Improper Protection of Alternate Path" - La ruta alternativa no está bien protegida
- **CWE-862**: "Missing Authorization" - Falta de autorización

Segunda Captura de Debilidades



Relationships

Relevant to the view "Research Concepts" (View-1000)

Nature	Type	ID	Name
ChildOf	B	288	Authentication Bypass Using an Alternate Path or Channel
ChildOf	C	424	Improper Protection of Alternate Path
ChildOf	C	862	Missing Authorization
CanPrecede	V	98	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion')
CanPrecede	B	471	Modification of Assumed-Immutable Data (MAID)

Relevant to the view "Software Development" (View-699)

Nature	Type	ID	Name
MemberOf	C	417	Communication Channel Errors
MemberOf	C	1212	Authorization Errors

Relevant to the view "Weaknesses for Simplified Mapping of Published Vulnerabilities" (View-1003)

Nature	Type	ID	Name
ChildOf	C	862	Missing Authorization

Relevant to the view "Architectural Concepts" (View-1008)

Nature	Type	ID	Name
MemberOf	C	1011	Authorize Actors

En esta segunda captura vemos más debilidades relacionadas:

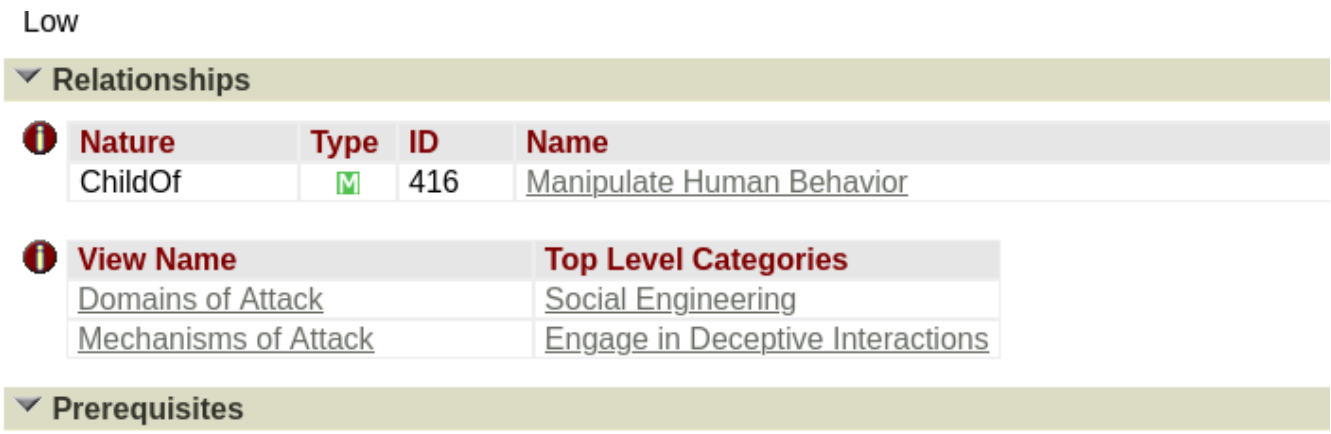
- **CWE-98**: Sobre inclusión remota de archivos
- **CWE-471**: Modificación de datos que se suponía que no podían cambiar
- **CWE-417**: Errores en canales de comunicación
- **CWE-1212**: Errores de autorización

Lo importante es que la mayoría señalan problemas con **autenticación y autorización**, que es el núcleo del problema.

---

6. Patrones de Ataque (CAPEC)

Cómo se explota la vulnerabilidad



Low

Relationships

Nature	Type	ID	Name
ChildOf	M	416	Manipulate Human Behavior

View Name	Top Level Categories
Domains of Attack	Social Engineering
Mechanisms of Attack	Engage in Deceptive Interactions

Prerequisites

En esta captura vemos el patrón de ataque CAPEC:

- **ID**: 416
- **Nombre**: "Manipulate Human Behavior"
- **Categoría**: Social Engineering
- **Dominios**: Social Engineering
- **Mecanismos**: Engage in Deceptive Interactions

Lo interesante es que aunque parece que es ingeniería social, lo que realmente sucede es que **se manipula el comportamiento del sistema para que haga algo que no debería**.

Se mencionan relaciones con otras debilidades como:

- **CWE-416**: Manipulate Human Behavior
- **CWE-288**: Authentication Bypass
- **CWE-424**: Improper Protection
- **CWE-862**: Missing Authorization

---

7. Análisis de Impacto

Esta vulnerabilidad afecta a:

Área	Impacto
Confidencialidad	Afectada - Se puede leer información del sistema
Integridad	Afectada - Se pueden modificar datos
Disponibilidad	Afectada - Se puede tomar control del sistema
Control de Acceso	Comprometido - Cualquiera puede ser administrador

---

9. Conclusión

Esta vulnerabilidad es **muy grave** porque permite a cualquiera acceder como administrador sin necesidad de contraseña. Afecta a todas las versiones de GoAnywhere MFT desde la 6.0.0 hasta la 7.4.0, pero ya tiene solución: actualizar a la 7.4.1 o aplicar los parches indicados.