Fortra GoAnywhere MFT Vulnerability

February 2024

SOC Informative Report

Document details

Title of the activity
Fortra GoAnywhere MFT Vulnerability

Summary
Report containing information about the vulnerability CVE-2024-0204, an authentication bypass in the Fortra GoAnywhere MFT service.

Target audience
SOC and SOC AdS representatives

Confidentiality level (Clear/Green/Amber/Amber+Strict/Red)
CLEAR

Publication date
05/02/2024

Written by
Mirko Ioris

Reviewed by
Massimo Giaimo

Confidentiality level

A level of confidentiality is applied to the document, marked by the "Confidentiality Level" item on the front page. The values that can be used (RED / AMBER / AMBER+STRICT / GREEN / CLEAR) have the following meanings:

TLP:RED = Reserved for participants only.

Sources may use TLP:RED when the information cannot be effectively used by other parties and could impact a party's privacy, reputation, or operations if misused. Recipients may not share TLP:RED information with parties outside the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most cases, TLP:RED should be exchanged verbally or in person.

TLP:AMBER = Limited disclosure, restricted to participants' organizations.

TLP:AMBER+STRICT limits sharing to the *organization* only.

Sources may use TLP:AMBER when the information requires support to act effectively but poses risks to privacy, reputation, or operations if shared outside the organizations involved. Recipients may share TLP:AMBER information only with members of their own organization and with clients or customers who need to know the information to protect themselves or prevent further harm.

Note: If the source wishes to limit sharing **only** to the organization, it must specify TLP:AMBER+STRICT.

TLP:GREEN =Limited disclosure, restricted to the community.

Sources may use TLP:GREEN when the information is useful for the awareness of all participating organizations, as well as with colleagues within the community or broader sector. Recipients may share TLP:GREEN information with colleagues and partner organizations within their sector or community, but not through publicly accessible channels. Information in this category may be widely disseminated within a particular community. TLP:GREEN information may not be released outside the community.

TLP:CLEAR = Disclosure is not limited.

Sources may use TLP:CLEAR when the information poses little or foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction.

Table of contents

Introduction

Fortra GoAnywhere MFT (Managed File Transfer) is a software used for secure file sharing between systems, employees, customers, and different companies.

The same service has already been in the spotlight last year, when it was targeted by the Cl0p ransomware group, which was able to exploit the zero-day vulnerability CVE-2023-0669 to breach 130 organizations worldwide [1].

This time, another critical CVE, tracked as **CVE-2024-0204**, is impacting the service.

NIST classification of the vulnerability [2]

Fortra released a security advisory on 22 January 2024 [3], revealing the critical vulnerability. The discovery date was 01 December 2023, and the vulnerability was patched a few days later with the release of **GoAnywhere MFT 7.4.1**. However, the company did not disclose any information at the time.

Overview of the attack

The **CVE-2024-0204** is an authentication bypass that allows an unauthorized user to create an admin user via the administration portal.

Researchers at Horizon3 published a Deep-Dive report [4] related to the vulnerability. We summarized it here below:

When installing GoAnywhere, the application will first direct users to the endpoint endpoint */InitialAccountSetup.xhtml* to set up a new **administrative user**.

After the configuration is completed, it's not possible to access the initial account configuration page again. If the user attempts to access this page, they are redirected either to the login form */auth/Login.xhtml* (if they are not authenticated), or to the welcome dashboard */Dashboard.xhtml*.

However, researchers discovered that it's possible to access the *InitialAccountSetup.xhtml* file again with a path traversal attempt containing the string */..;/*.

Thus, making a request to a vulnerable URL like this:

https://IP:PORT/goanywhere/images/...;/wizard/InitialAccountSetup.xhtml

allows anyone to access the initial configuration page and create a new user account with administrator privileges.

As proof of the attack's feasibility, researchers wrote and published a **Proof-of-Concept** (PoC) exploit, capable of creating an administrator account in vulnerable versions of GoAnywhere MFT. The PoC is available on GitHub [5].

All a cybercriminal needs in order to exploit the vulnerability is to specify a new account name, a password and the vulnerable endpoint.

Remediation

The affected versions of the product are the following:

- Fortra GoAnywhere MFT 6.x from 6.0.1
- Fortra GoAnywhere MFT 7.x before 7.4.1

Upgrading to version 7.4.1 or higher will successfully remove the vulnerability.

Workarounds

According to Fortra's advisory, the vulnerability may also be eliminated in these ways:

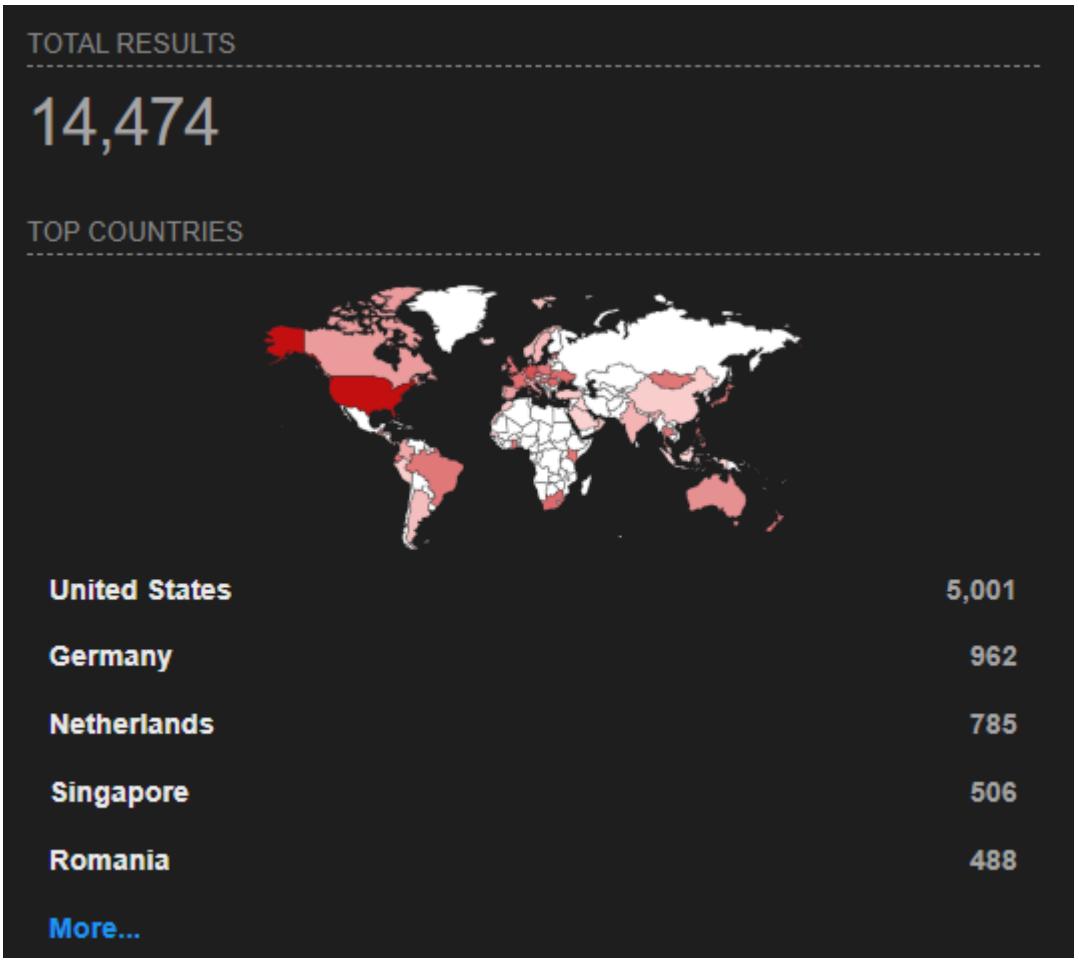
- For non-container deployments, delete the `InitialAccountSetup.xhtml` file in the installation directory and restart the services,
- For container-deployed instances, delete the `InitialAccountSetup.xhtml` file in the installation directory and replace it with an empty file, then restart the services.

Attack surface

Using a device search engine such as **Shodan**, it is possible to check the amount of devices that expose a GoAnywhere Web client on the Internet and are publicly reachable.

Below are the devices found with the Shodan query (search date 05/02/2024):

Shodan Query
html:"InvalidBrowser.xhtml"



IOCs

- Review the **Admin Users group** in the administrative console and look for new additions. If the attacker's account is present, you may be able to see its last logon activity.

- Review **database logs** and look for entries indicating new user creation.
    - *\GoAnywhere\userdata\database\goanywhere\log*.log*

Bibliography

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

[2]https://nvd.nist.gov/vuln/detail/CVE-2024-0204

[3]https://www.fortra.com/security/advisory/fi-2024-001

[4]https://www.horizon3.ai/cve-2024-0204-fortra-goanywhere-mft-authentication-bypass-deep-dive/

[5]https://github.com/horizon3ai/CVE-2024-0204