



| Flash |

Fortra Discloses Critical MFT Vulnerability

F-2024-01-24a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Ransomware, Vulnerability Exploitation

January 24, 2024

Scope Note: ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 9:00 AM (EST) on January 24, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Fortra Discloses Critical MFT Vulnerability

› Key Findings

- On January 22, 2024, Fortra publicly disclosed a critical authentication bypass flaw in its GoAnywhere managed file transfer (MFT) software, for which a security patch has been released to end users.
- Although no active exploitation in the wild has been observed as of this writing, recent public disclosure and the publication of a proof-of-concept (PoC) suggests that attacks against unpatched systems are very likely.
- In Q1 2023, the C10p extortion collective successfully exploited a zero-day vulnerability in Fortra's MFT software in what became one of the most widespread and lucrative Ransomware & Digital Extortion (R&DE) campaigns of the year.

| Details

On January 22, 2024, Fortra publicly disclosed CVE-2024-0204, a critical authentication bypass flaw in its MFT software. CVE-2024-0204 enables unauthenticated threat actors to create a new admin account with full privileges without requiring any credentials. Successful exploitation of the vulnerability can facilitate data theft, deployment of malicious payloads such as ransomware, and lateral movement.

- The vulnerability enables threat actors to bypass authentication checks to access the admin account creation page by exploiting a path traversal vulnerability in the /InitialAccountSetup.xhtml endpoint.
- The vulnerability has been assigned a critical CVSS score of 9.8 out of 10.
- The exploit impacts Fortra GoAnywhere MFT version 6.x from 6.0.1 onwards and versions 7.x prior to 7.4.1.

Fortra released a security patch on December 7, 2023, in v.7.4.1. Fortra privately notified customers as early as December 4, 2023, of the existence of the vulnerability. Customers were advised to patch immediately.¹

While no active exploitation in the wild has been observed, the recent public disclosure of the vulnerability coupled with the fact that security researchers have published a PoC suggests that attacks in the wild against unpatched systems are very likely. The PoC contains just 10 lines of code.

```
% python3 CVE-2024-0204.py -h
usage: CVE-2024-0204 GoAnywhere Authentication Bypass [-h]
                                     endpoint username
                                     password

positional arguments:
  endpoint      The endpoint URL (e.g., http://127.0.0.1:8080)
  username      New admin username
  password      New admin password

optional arguments:
  -h, --help    show this help message and exit
```

PoC for CVE-2024-0204: Authentication Bypass in GoAnywhere MFT

Source: [hXXps://github\[.\]com/horizon3ai/CVE-2024-0204?ref=thestack.technology](https://github.com/horizon3ai/CVE-2024-0204?ref=thestack.technology)

ZeroFox urges users that have not already updated to a secure version (7.4.1 or higher) to implement the patch immediately. For those unable to update, Fortra has issued two manual mitigation paths:

¹ [hXXps://www.fortra\[.\]com/security/advisory/fi-2024-001](https://www.fortra.com/security/advisory/fi-2024-001)

- Delete the InitialAccountSetup.xhtml file in the installation directory and restart the service.
- Replace the InitialAccountSetup.xhtml file with an empty file and restart the service.

In Q1 2023, the Cl0p extortion collective successfully exploited a zero-day vulnerability (later assigned CVE-2023-0669) in Fortra's MFT software. The pre-authentication command injection vulnerability enabled Cl0p to successfully extort over 130 organizations in what became one of the year's most widespread and lucrative R&DE campaigns; Cl0p is reported to have likely generated up to USD 100,000,000 in revenue.²³

It is very unlikely that the exploitation of CVE-2024-0204 will be as widespread or as lucrative for threat actors as CVE-2023-0669. However, threat actors will very likely seek to exploit this latest vulnerability en masse in the short term.

- CVE-2023-0669 was exploited as a zero-day vulnerability, allowing exploitation to take place before a mitigating software patch could be released.
- Cl0p's initial exploitation of CVE-2023-0669 primarily targeted on-premises infrastructure, which likely enabled significantly more subsequent exploitation.

| Recommendations

- Ensure networks are patched with the latest GoAnywhere MFT version 7.41 or higher, as described above.
 - [hXXps://www.fortra\[.\]com/security/advisory/fi-2024-001?ref=thetack.technology](https://www.fortra[.]com/security/advisory/fi-2024-001?ref=thetack.technology)
- If unable to implement the security patch, employ the manual mitigation paths described above.
- Monitor system logs for any suspicious admin account creation activity, including new additions to the Admin Users group in the GoAnywhere administrator portal

²

[hXXps://www.bleepingcomputer\[.\]com/news/security/cl0p-ransomware-claims-it-breached-130-orgs-using-goanywhere-zero-day/](https://www.bleepingcomputer[.]com/news/security/cl0p-ransomware-claims-it-breached-130-orgs-using-goanywhere-zero-day/)

³

[hXXps://www.coveware\[.\]com/blog/2023/7/21/ransom-monetization-rates-fall-to-record-low-despite-jump-in-average-ransom-payments](https://www.coveware[.]com/blog/2023/7/21/ransom-monetization-rates-fall-to-record-low-despite-jump-in-average-ransom-payments)

“Users – Admin Users” section. Additionally, review logs for the database `\GoAnywhere\userdata\database\goanywhere\log\*.log` for the creation of additional users.

- Ensure a thorough understanding of organizational technology stacks, including those of operating partners.
- Consistently monitor for security patch releases impacting this product, and deploy a holistic patch management system to ensure all business IT assets are updated with the latest software as quickly as possible.
- Leverage CISA’s KEV catalog to prioritize out-of-cycle vulnerability patching.
- Protect endpoint devices with phishing-resistant multi-factor authentication (MFA) protocols compliant with FIDO2 or PKI standards.
- Ensure critical data is backed up to secure off-site or cloud servers. Sensitive or proprietary data should be properly compartmentalized, avoiding aggregation or unnecessary accumulation.
- Use the ZeroFox Platform’s Intelligence Search capability to investigate vulnerabilities and associated exploits.
- Maintain a clear and comprehensive incident response strategy consisting of business resilience and continuity plans, incident reporting procedures, and key authorities.

Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.

| Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%