Hackers exploit Fortra GoAnywhere flaw before public alert

Data: 2025-09-26 15:00:06

Autor: Inteligência Against Invaders

Hackers exploit Fortra GoAnywhere flaw before public alert

watchTowr Labs says hackers exploited the Fortra GoAnywhere MFT flaw CVE-2025-10035 on Sept 10, 2025, a week before public disclosure.

Cybersecurity firm watchTowr Labs revealed that it has ‘credible evidence’ that the critical Fortra GoAnywhere MFT flaw CVE-2025-10035 was actively exploited in attacks in the wild as early as September 10, 2025, a week before it was publicly disclosed.

Fortra GoAnywhere Managed File Transfer is a comprehensive solution for secure file transfer, data encryption, and compliance management. It provides a centralized platform for managing and automating file transfers between disparate systems and applications, enabling secure and controlled data movement across an organization’s network.

On September 18, Fortra addressed a critical vulnerability, tracked as CVE-2025-10035 (CVSS score of 10.0) in GoAnywhere Managed File Transfer (MFT) software.

The flaw is a deserialization vulnerability in the License Servlet of Fortra’s GoAnywhere MFT. An attacker could exploit the vulnerability to execution of arbitrary commands on the affected systems.

*“A deserialization vulnerability in the License Servlet of Fortra’s GoAnywhere MFT allows an actor with a validly forged license response signature to deserialize an arbitrary actor-controlled object, possibly leading to command injection.”*reads the advisory*.*

The company urges customers to upgrade to a patched version (the latest release 7.8.4, or the Sustain Release 7.6.3).

To mitigate the vulnerability, Fortra recommends restricting public access to the GoAnywhere Admin Console, as exploitation depends on internet exposure.

*“We have been given credible evidence of in-the-wild exploitation of Fortra GoAnywhere CVE-2025-10035 dating back to September 10, 2025. That is eight days before Fortra’s public advisory,”*watchTower notes*. “That is eight days before Fortra’s public advisory, published September 18, 2025. This explains why Fortra later decided to publish limited IOCs, and we’re now urging defenders to immediately change how they think about timelines and risk. An individual sent us evidence of exploitation activity that aligns with the stack traces shown in Fortra’s advisory.”*

watchTowr found over 20,000 internet-facing GoAnywhere MFT instances, including Fortune 500.

Cybersecurity firm Rapid7 also states that the flaw involves a chain of three bugs, it is a not simple deserialization issue.

*“The following analysis details our current understanding of the vulnerability, and finds that the issue, as described by the vendor,**is not just a single deserialization vulnerability, but rather a chain of three separate issues**. This includes an access control bypass that has been known since 2023, the unsafe deserialization vulnerability CVE-2025-10035, and an as-yet unknown issue pertaining to how the attackers can know a specific private key.”* states Rapid7*. “As of September 24, 2025, there is no known exploit code publicly available, and the vendor has not indicated the vulnerability as having been exploited in-the-wild, although the vendor advisory has been updated to include IOCs, which is unusual for a vulnerability that has not been exploited in-the-wild.”*

Follow me on Twitter:@securityaffairsandFacebookandMastodon

PierluigiPaganini

(SecurityAffairs–hacking, Fortra)