It Is Bad (Exploitation of Fortra GoAnywhere MFT CVE-2025-10035) - Part 2

Ryan Dewhurst ⋮ ⋮ 9/25/2025

By — Ryan Dewhurst — Sonny — Sep 25, 2025


It Is Bad (Exploitation of Fortra GoAnywhere MFT CVE-2025-10035) - Part 2

We're back, just over 24 hours later, to share our evolving understanding of CVE-2025-10035.

Thanks to everyone who reached out after Part 1, and especially to the individual who shared credible intel that informed this update.

In **Part 1** we laid out an odd and worrying picture:

- A vendor advisory that included an "Am I Impacted?" section with what looked like a stack trace from attempted exploitation,
- A vendor that has publicly signed the Secure By Design pledge, committing to transparency around in-the-wild exploitation, and,
- A carefully worded statement suggesting the issue was found during an internal "security check" on September 11, 2025.

It'd be understandable if you interpreted all of this as "we discovered this vulnerability internally ourselves."

CYBERSCOOP Topics Special Reports Events Podcasts Videos

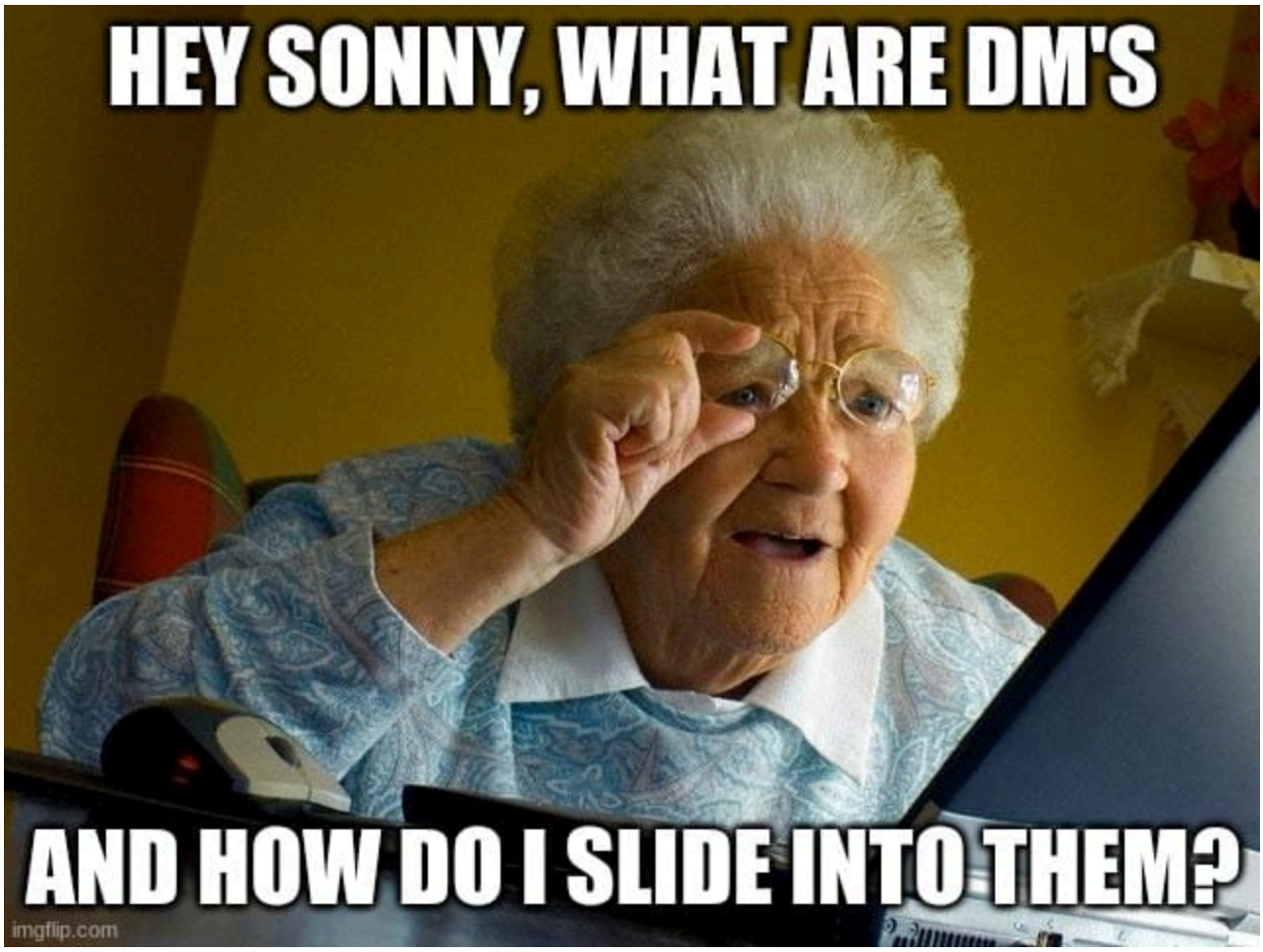
> Fortra told CyberScoop it discovered the vulnerability during a security check Sept. 11. "We identified that GoAnywhere customers with an admin console accessible over the internet could be vulnerable to unauthorized third-party exposure," Jessica Ryan, public relations manager at Fortra, said in an email.
>
> "We immediately developed a patch and offered customers mitigation guidance to help resolve the issue," she added.

You'd also seemingly be wrong, and welcome to Part 2.

Since Part 1…

Since Part 1, 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, 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.



The stack trace related to exploitation, and the creation of a backdoor account, are both present in the data we reviewed. We cannot publish everything, but the core signals are clear.

Observed Exploitation and Post-Exploitation Activities

Below, we have summarised the sequence of exploitation and follow-on activity observed in-the-wild.

1. The threat actor triggers the **pre-auth deserialization** vulnerability in GoAnywhere MFT, achieving Remote Code Execution (RCE).
2. With the RCE, they create an GoAnywhere user, a backdoor admin account named *admin-go*.
3. Using the *admin-go* account, they create a **web user.** Now they have "legitimate" access to the solution itself.
4. Via that new web user, the threat actor uploads and executes multiple secondary payloads.

Indicators of Compromise (or as Fortra probably calls them, “Indicators of Impact”)

Unfortunately, the picture now painted allows for evidence-based confidence in the concern that Fortra’s “Am I Impacted?” section probably was not Fortra attempting to be overly helpful, but a thinly veiled way of sharing “Indicators of Compromise”.

We can all stop lying to ourselves - please.

Below, we are sharing the IoCs shared within the evidence we received for in-the-wild exploitation of CVE-2025-10035.

Type	Value	Description
File	C:\Windows\zato_be.exe	Likely second stage implant
SHA-256	68c4abcb024c65388db584122eff409fb8459e0ca930c717f2217b90e6f2f5bc	Hash of `zato_be.exe`
File	C:\Windows\jwunst.exe	SimpleHelp binary observed in activity
SHA-256	a72fa3b5bdd299579a03b94944e2b0b18f1bf564d4ff08a19305577a27575cc8	Hash of `jwunst.exe`
Local account	admin-go	Created backdoor user
IPv4 address	155[.]2[.]190[.]197	Observed actor IP address
Command	whoami /groups	Command run by actor
File	C:\Windows\test.txt	File containing output of `whoami /groups`

Sigh

This is an increasingly disappointing situation: Fortra had the chance to honour the Secure By Design pledge and be transparent about in-the-wild exploitation, but instead, they decided otherwise...

The reality is simple: this leaves security teams scrambling to assess risk and decide whether to assume continued exposure or to treat this as a prompt for a full incident response and forensic review.

Please, just be transparent - what an unnecessary saga.

The research published by watchTowr Labs is just a glimpse into what powers the watchTowr Platform – delivering automated, continuous testing against real attacker behaviour.

By combining Proactive Threat Intelligence and External Attack Surface Management into a single **Preemptive Exposure Management** capability, the watchTowr Platform helps organisations rapidly react to emerging threats – and gives them what matters most: **time to respond.**

Gain early access to our research, and understand your exposure, with the watchTowr Platform

REQUEST A DEMO