Maximum severity GoAnywhere MFT flaw exploited as zero day - Against I

Data: 2025-09-26 15:36:51

Autor: Inteligência Against Invaders

Hackers are actively exploiting a maximum severity vulnerability (CVE-2025-10035) in Fortra's

GoAnywhere MFT that allows injecting commands remotely without authentication.

The vendor disclosed the flawon September 18, buit the company had learned about it a week earlier, and did not share any details on how it was discovered or if it was being exploited.

CVE-2025-10035 is a deserialization vulnerability inthe License Servlet of the GoAnywhere managed file transfer software that can be leveraged to inject commands by "an actor with a validly forged license response signature."

Although Fortra's advisory hasn't been updated to include any information about the vulnerabililty being used in attacks, security researchers at WatchTowr Labs say that they received "credible evidence" ofFortra GoAnywhere CVE-2025-10035 being leveraged as a zero day.

"We have been given credible evidence of in-the-wild exploitation of Fortra GoAnywhere CVE-2025-10035 dating back to September 10, 2025," reads WatchTowr's report.

"That is eight days before Fortra's public advisory, published September 18, 2025," the researchers point out.

"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."

WatchTowr confirmed that the analyzed data contains the stack trace related to exploitation and the creatiuon of a backdoor account:

1. achievingremote command execution after exploiting the pre-auth deserialization vulnerability
2. creating a backdoor admin account called*admin-go*
3. using the account to create a web user that enabled "legitimate" access
4. uploadingand executingmultiple secondary payloads

From the indicators of compromise WatchTowr published at the bottom of the report, the payloads are named '*zato_be.exe*' and '*jwunst.exe*.'

The latter is a a legitimate binary for the remote access product SimpleHelp. In this case, it is being abused for persistent hands-on control of the compromised endpoints.

The researchers also note that the attackers executed the '*whoami/groups*' command, which prints the current user account and Windows group memberships, and saved the output to a text file

(*test.txt*) for exfiltration.

This allows the threat actor to check the privileges of the compromised account and explore lateral movement opportunities within the breached environment.

[IMAGEM REMOVIDA]also recommendsthat admins inspect log files for errors containing the string”SignedObject.getObject,’ to determine if an instance has been impacted.

[IMAGEM REMOVIDA]