Fortra GoAnywhere Vuln Exploited as 0-Day Before Patch – InfoSecBulleti

Data: 2025-09-27 07:36:07

Autor: Inteligência Against Invaders

A critical vulnerability with a perfect 10.0 CVSS score in Fortra's GoAnywhere Managed File

Transfer (MFT) solution was exploited as a zero-day for at least a week before a patch was released.

CVE-2025-10035 is a command injection vulnerability enabling remote code execution without authentication. Security firm watchTowr noted evidence of active exploitation since September 10, 2025, just before Fortra's advisory on September 18.

Fortra initially described the vulnerability as a deserialization issue in the GoAnywhere MFT License Servlet. According to the vendor's advisory, an attacker with a "validly forged license response signature" could deserialize a crafted object, leading to command injection.

Fortra announced on September 18 that an issue was discovered during an internal security check on September 11, but did not mention any active exploitation, which researchers found unusual given the Indicators of Compromise (IoCs) included.

Vulnerability Exploited as 0-Day:

Security researchers have explained the flaw and how it was exploited.

Research from Rapid7 ***shows*** that CVE-2025-10035 is a combination of three issues: an access control bypass from 2023, a new unsafe deserialization flaw, and an unknown problem that lets attackers access a certain private key for the exploit.

Threat actors exploited the pre-authentication deserialization vulnerability to achieve Remote Code Execution (RCE).

Attackers created a backdoor admin account called admin-go, which they used to set up a legitimate web user account for MFT service access. They then uploaded and ran multiple secondary payloads through this account.

WatchTowr Labs reported that the exploitation began on September 10, before the patch was released on September 15 and the public advisory on September 18, confirming it as a zero-day vulnerability.

Fortra, a signatory of the Secure By Design pledge, faces criticism for not disclosing active attacks. This left security teams without a complete understanding of the threat timeline for risk assessment.

Indicators of Compromise (IoCs):

Evidence of the in-the-wild attacks includes several key indicators:

Backdoor Account: A local account named admin-go was created on compromised systems.

Malicious Files: Payloads such as C:Windowszato_be.exe and C:Windowsjwunst.exe (a SimpleHelp binary) were observed.

Attacker IP: The IP address 155.2.190.197 was linked to the threat actor.

Commands Executed: The command whoami /groups was run, with its output saved to C:Windowstest.txt.

Fortra has ***released*** GoAnywhere MFT version 7.8.4 and Sustain version 7.6.3 to address the vulnerability.

Given the history of GoAnywhere MFT being targeted by ransomware groups, organizations are urged to patch immediately and ensure their admin consoles are not exposed to the public internet.