GoAnywhere MFT Flaw Opens Door to Remote Command Execution

TL;DR

Fortra released patches for CVE-2025-10035, a CVSS 10.0 deserialization vulnerability in GoAnywhere MFT.

If the Admin Console is internet-facing, attackers could exploit this flaw to execute arbitrary commands. Update to 7.8.4 or Sustain Release 7.6.3, or restrict access immediately.

Overview

A critical vulnerability (CVE-2025-10035, CVSS 10) was found in in the License Servlet of Fortra's GoAnywhere MFT. The flaw allows a forged license response signature to deserialize attacker-controlled objects, allowing for command injection without authentication or user interaction. Internet-facing Admin Consoles are at highest risk.

CVE-2025-10035 is a deserialization flaw in GoAnywhere MFT's License Servlet that can be triggered with a forged license response. Successful exploitation results in arbitrary command execution. The vulnerability affects all versions through 7.8.3.

GoAnywhere has a track record of exploitation by ransomware groups. With this flaw rated at the maximum CVSS score, Aspire recommends patching and isolating exposed systems immediately.

Aspire Protects

- **Patch** – upgrade to GoAnywhere MFT 7.8.4 or Sustain Release 7.6.3.
- Make sure the Admin Console is not exposed to the internet until patched.
- Review firewall and access rules for unnecessary exposure.
- Investigate suspicious License Servlet requests or command activity.

TTPs to Watch

Initial Access

- Exploit Public-Facing Application [T1190] – The attacker may exploit an internet-facing Admin Console to trigger the flaw.

Execution

- Command and Scripting Interpreter [T1059] – The attacker may run arbitrary commands after exploitation.

Persistence

- Create or Modify System Process [T1543] – The attacker may establish long-term access by modifying system processes.

Impact

- Data Destruction [T1485] – The attacker may delete or corrupt transferred files or logs through executed commands.

IoCs

There are no known IoCs associated with the above vulnerability at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

The GoAnywhere MFT vulnerability threatens any organization using the platform for secure file transfers and audit logging.

- Education
- Energy
- Finance
- Healthcare
- Retail
- Manufacturing

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

CWE - CWE-502: Deserialization of Untrusted Data (4.18)

CVE Record: CVE-2025-10035

Deserialization Vulnerability in GoAnywhere MFT's License Servlet | Fortra