CALIFORNIA CYBERSECURITY INTEGRATION CENTER

CYBER ADVISORY

Friday, October 10, 2025 **CSIC-ADVISORY-202510-A-002**

Fortra's GoAnywhere MFT: Critical RCE

Medusa Ransomware | Deserialization Flaw | CVE-2025-10035 | Storm-1175

SUMMARY: The Cybersecurity Integration Center (CSIC) has identified a critical vulnerability (CVE-2025-10035) affecting Fortra GoAnywhere Managed File Transfer (MFT), a core component used for secure data exchange. Rated 10.0 (Critical)[1] on the CVSS v3.1 scale, the vulnerability is a deserialization of untrusted data flaw (CWE-502) within the software's License Servlet (Administrative Console). This flaw allows a remote, unauthenticated attacker to forge a license response signature and deserialize an arbitrary, actor-controlled object, leading to Remote Code Execution (RCE) and potential command injection (CWE-77)[2] on the MFT application. Active exploitation of this zero-day has been observed in the wild, linked to the threat group Storm-1175, a Microsoft-tracked financially motivated threat group known for deploying Medusa ransomware.[3] Public detection resources and Proof-of-Concept (PoC) code are available, which may increase the attack surface and speed up exploitation attempts.[4]

Affected Versions (CVE-2025-10035):

- Fortra GoAnywhere MFT, versions prior to 7.6.3
- Fortra GoAnywhere MFT, versions from 7.7.0 and up (excluding 7.8.4)

The Cal-CSIC recommends upgrading to one of the patched versions of Fortra as soon as possible. Please refer to the Fortra Security Advisory detailing the RCE vulnerability, for further information and resources.

References

[1] National Vulnerability Database; "CVE-2025-10035 Detail"; https://nvd.nist.gov/vuln/detail/CVE-2025-10035; accessed 09 October 2025

[2] Fortra; "Deserialization Vulnerability in GoAnywhere MFT's License Servlet"; https://www.fortra.com/security/advisories/product-security/fi-2025-012; accessed 09 October 2025

[3] Microsoft Security Blog; "Investigating active exploitation of CVE-2025-10035 GoAnywhere Managed File Transfer vulnerability"; https://www.microsoft.com/en-us/security/blog/2025/10/06/investigating-active-exploitation-of-cve-2025-10035-goanywhere-managed-file-transfer-vulnerability/; accessed 09 October 2025

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

[4] rxerium; "CVE-2025-10035: Detection for CVE-2025-10035"; https://github.com/rxerium/CVE-2025-10035; accessed 09 October 2025

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.