مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical RCE Vulnerability in GoAnywhere MFT
Tracking #:432317736
Date:22-09-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Fortra has released an advisory regarding a critical deserialization vulnerability (CVE-2025-10035) in its GoAnywhere Managed File Transfer (MFT) solution.

TECHNICAL DETAILS:

Fortra has released an advisory regarding a critical deserialization vulnerability (CVE-2025-10035) in its GoAnywhere Managed File Transfer (MFT) solution. The flaw resides in the License Servlet component and allows an attacker to achieve unauthenticated remote code execution (RCE) by forging a malicious license response.

The vulnerability carries a CVSS v3.1 score of 10.0 (Critical) and, if exploited, could allow complete compromise of affected systems, including exfiltration of sensitive data, deployment of malware, or lateral movement within enterprise networks.

Vulnerability Details:
- **CVE ID:** CVE-2025-10035
- **CVSS v3.1 Score:** 10.0
- **Severity:** Critical

Affected Products:
- **GoAnywhere MFT**
  - Versions prior to **7.8.4** (latest release)
  - Sustain Release branch prior to **7.6.3**

Mitigation:
- Restrict Access:
  - Ensure the GoAnywhere Admin Console is not exposed to the public internet. Restrict access to trusted internal networks or via VPN only.

- Apply Security Patches: Upgrade to one of the following patched versions immediately:
  - 7.8.4 (Latest Release)
  - 7.6.3 (Sustain Release)

RECOMMENDATIONS:

- All organizations using GoAnywhere MFT must immediately patch to fixed version and restrict Admin Console exposure to minimize risk of exploitation.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

REFERNCES:

- https://www.fortra.com/security/advisories/product-security/fi-2025-012