Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Storm-1175's Masterstroke Exploits CVE-2025-10035 in GoAnywhere MFT

Date of Publication	Admiralty Code	TA Number
October 17, 2025	A1	TA2025319

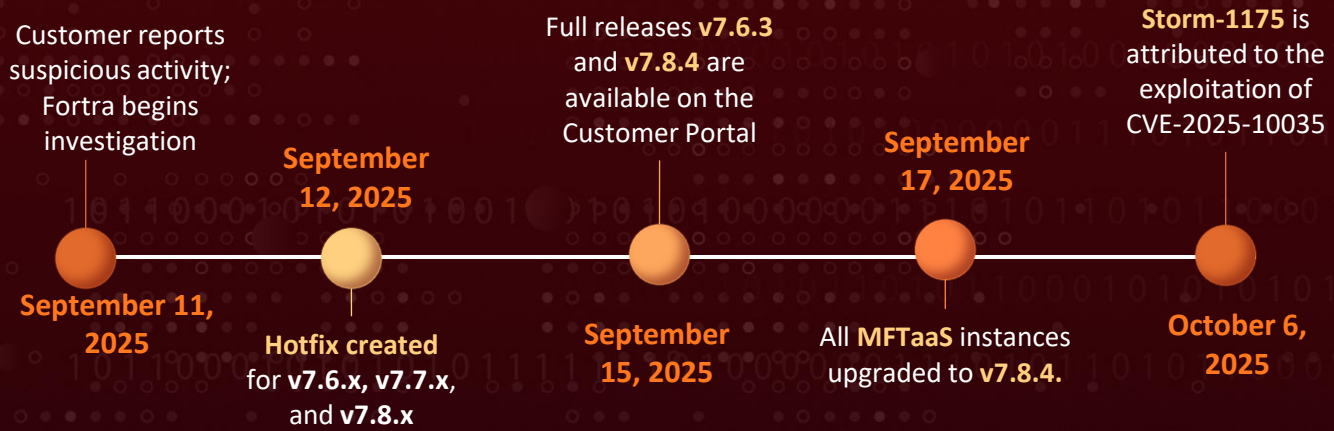
Summary

Active Exploitation: September 2025
Affected Product: GoAnywhere MFT
Threat Actor: Storm-1175
Malware: Medusa ransomware
Impact: CVE-2025-10035 is a critical deserialization vulnerability in Fortra's GoAnywhere Managed File Transfer (MFT) that was actively exploited by the cybercriminal group Storm-1175 in September 2025. Affecting GoAnywhere MFT (Admin Console) versions up to 7.8.3, the flaw allows attackers to bypass license-signature verification by submitting a forged license response, trigger deserialization of attacker-controlled objects, and achieve remote code execution (RCE), enabling a full system compromise that Storm-1175 used to deploy the Medusa ransomware.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-10035	Fortra GoAnywhere MFT Deserialization of Untrusted Data Vulnerability	GoAnywhere MFT	✓	✓	✓

Exploitation Timeline



Vulnerability Details

#1 CVE-2025-10035 is a critical deserialization vulnerability in the License Servlet of Fortra's GoAnywhere Managed File Transfer (MFT) that was assessed to be under active exploitation in September 2025. An attacker capable of producing a validly forged license-response signature can force the servlet to deserialize an attacker-controlled object, enabling command injection and potential remote code execution (RCE).

#2 The flaw affects GoAnywhere MFT Admin Console versions up to 7.8.3 and allows bypass of signature verification by submitting a crafted, forged license response. Exploitation can occur without authentication if an attacker can craft or intercept such license responses, making internet-exposed instances especially high risk.

#3 A cybercriminal group tracked as **Storm-1175**, known for deploying ransomware and exploiting public-facing applications, was observed exploiting this zero-day. For initial access, they leveraged the deserialization bug. To maintain persistence, they abused remote monitoring and management (RMM) tools SimpleHelp and MeshAgent, placing RMM binaries beneath the GoAnywhere MFT process and creating .jsp files inside GoAnywhere directories concurrently.

#4 Post-compromise activity included user and system discovery, network scanning (netscan), and lateral movement using mstsc.exe. The actors utilized RMM tools for command-and-control and established a Cloudflare tunnel for secure command and control. Data exfiltration activity included the deployment and execution of Rclone in at least one victim environment. Medusa ransomware was successfully deployed in one observed compromise.

#5 Fortra released GoAnywhere versions 7.6.3 and 7.8.4 to remediate the vulnerability. In a related historical note, the Cl0p ransomware gang claimed in 2023 to have exploited **CVE-2023-0669**, a pre-auth command-injection vulnerability in the Licensing Response Servlet of GoAnywhere MFT and asserted breaches of more than 130 organizations.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-10035	GoAnywhere MFT Versions up to and including 7.8.3	cpe:2.3:a:fortra:goanywhere_managed_file_transfer:*:*:*:*:*:*:*:*	CWE-77 CWE-502

Recommendations

Upgrade to Patched Versions: Apply the latest GoAnywhere MFT releases: v7.8.4 for current production and MFTaaS instances, or v7.6.3 for Sustain Release users. Verify that all instances, including MFTaaS, have been upgraded to prevent exploitation of CVE-2025-10035.

Restrict Admin Console Access: Remove GoAnywhere Admin Console from public internet exposure. Limit access to trusted internal networks or via secure VPN connections. Configure perimeter firewalls and proxies to prevent arbitrary internet connections, reducing the risk of malware downloads and command-and-control activity.

Monitor Audit Logs: Regularly review Admin Audit logs for suspicious activity, specifically in the userdata/logs/ directory. Inspect logs for errors containing SignedObject.getObject or license parsing exceptions, which may indicate potential exploitation. Configure firewalls, proxies, and network segmentation to prevent servers from making arbitrary outbound connections.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0007 Discovery	TA0008 Lateral Movement	TA0010 Exfiltration	TA0040 Impact
TA0011 Command and Control	T1588.006 Vulnerabilities	T1190 Exploit Public-Facing Application	T1078 Valid Accounts
T1059 Command and Scripting Interpreter	T1133 External Remote Services	T1505.003 Web Shell	T1213 Data from Information Repositories
T1082 System Information Discovery	T1046 Network Service Discovery	T1021.001 Remote Desktop Protocol	T1090 Proxy

T1133	T1567.002	T1041	T1486
External Remote Services	Exfiltration to Cloud Storage	Exfiltration Over C2 Channel	Data Encrypted for Impact

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	4106c35ff46bb6f2f4a42d63a2b8a619f1e1df72414122ddf6fd1b1a644b3220, c7e2632702d0e22598b90ea226d3cde4830455d9232bd8b33ebcb13827e99bc3, cd5aa589873d777c6e919c4438afe8bceccad6bbe57739e2ccb70b39aee1e8b3, 5ba7de7d5115789b952d9b1c6cff440c9128f438de933ff9044a68fff8496d19
IPv4	31[.]220[.]45[.]120, 45[.]11[.]183[.]123, 213[.]183[.]63[.]41

Patch Details

Apply the patch immediately by upgrading to the latest fixed version: 7.8.4 (latest release) or 7.6.3 (Sustain Release).

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

References

https://www.fortra.com/blog/summary-investigation-related-cve-2025-10035

https://www.microsoft.com/en-us/security/blog/2025/10/06/investigating-active-exploitation-of-cve-2025-10035-goanywhere-managed-file-transfer-vulnerability/

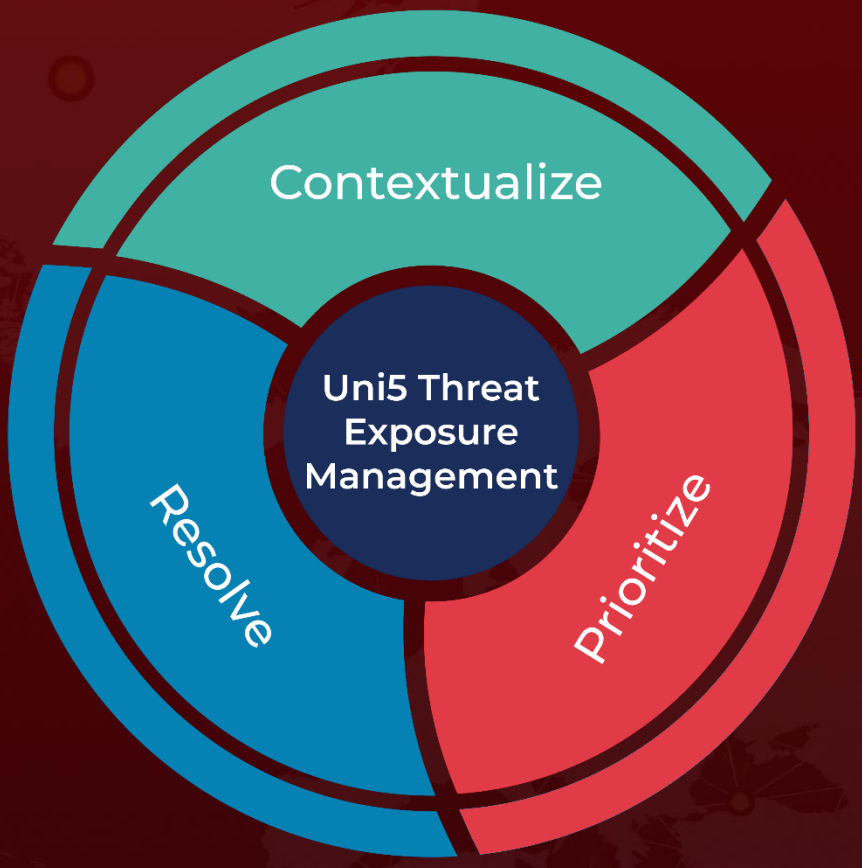
https://hivepro.com/threat-advisory/vmware-esxis-fatal-flaw-cve-2024-37085-opens-doors-for-ransomware-havoc/

https://hivepro.com/threat-advisory/clop-ransomware-group-claims-responsibility-for-goanywhere-mft-attacks/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

October 17, 2025 . 08:30 AM

More at www.hivepro.com