Investigating active exploitation of CVE-2025-10035 GoAnywhere Managed File Transfer vulnerability

By Microsoft Threat Intelligence ⋮ ⋮ 10/6/2025

On September 18, 2025, Fortra published a security advisory regarding a critical deserialization vulnerability in GoAnywhere MFT's License Servlet, which is tracked as CVE-2025-10035 and has a CVSS score of 10.0. The vulnerability could allow a threat actor with a validly forged license response signature to deserialize an arbitrary actor-controlled object, possibly leading to command injection and potential remote code execution (RCE). A cybercriminal group tracked by Microsoft Threat Intelligence as Storm-1175, known for deploying Medusa ransomware and exploiting public-facing applications for initial access, was observed exploiting the vulnerability.

Microsoft urges customers to upgrade to the latest version following Fortra's recommendations. We are publishing this blog post to increase awareness of this threat and to share end-to-end protection coverage details across Microsoft Defender, as well as security posture hardening recommendations for customers.

Vulnerability analysis

The vulnerability, tracked as CVE-2025-10035, is a critical deserialization flaw impacting GoAnywhere MFT's License Servlet Admin Console versions up to 7.8.3. It enables an attacker to bypass signature verification

by crafting a forged license response signature, which then allows the deserialization of arbitrary, attacker-controlled objects.

Successful exploitation could result in command injection and potential RCE on the affected system. Public reports indicate that exploitation does not require authentication if the attacker can craft or intercept valid license responses, making this vulnerability particularly dangerous for internet-exposed instances.

The impact of CVE-2025-10035 is amplified by the fact that, upon successful exploitation, attackers could perform system and user discovery, maintain long-term access, and deploy additional tools for lateral movement and malware. Public advisories recommend immediate patching, reviewing license verification mechanisms, and closely monitoring for suspicious activity in GoAnywhere MFT environments to mitigate risks associated with this vulnerability.

Exploitation activity by Storm-1175

Microsoft Defender researchers identified exploitation activity in multiple organizations aligned to tactics, techniques, and procedures (TTPs) attributed to Storm-1175. Related activity was observed on September 11, 2025.

An analysis of the threat actor's TTPs reveals a multi-stage attack. For initial access, the threat actor exploited the then-zero-day deserialization vulnerability in GoAnywhere MFT. To maintain persistence, they abused remote monitoring and management (RMM) tools, specifically SimpleHelp and MeshAgent. They dropped the RMM binaries directly under the GoAnywhere MFT process. In addition to these RMM payloads, the creation of *.jsp* files within the GoAnywhere MFT directories was observed, often at the same time as the dropped RMM tools.

The threat actor then executed user and system discovery commands and deployed tools like netscan for network discovery. Lateral movement was achieved using *mstsc.exe*, allowing the threat actor to move across systems within the compromised network.

For command and control (C2), the threat actor utilized RMM tools to establish their infrastructure and even set up a Cloudflare tunnel for secure C2 communication. During the exfiltration stage, the deployment and execution of Rclone was observed in at least one victim environment. Ultimately, in one compromised environment, the successful deployment of Medusa ransomware was observed.

Mitigation and protection guidance

Microsoft recommends the following mitigations to reduce the impact of this threat.

- Upgrade to the latest version following Fortra's recommendations. Note that upgrading does not address previous exploitation activity, and review of the impacted system may be required.
- Use an enterprise attack surface management product, like Microsoft Defender External Attack Surface Management (Defender EASM), to discover unpatched systems on your perimeter.

- Check your perimeter firewall and proxy to ensure servers are restricted from accessing the internet for arbitrary connections, like browsing and downloads. Such restrictions help inhibit malware downloads and command-and-control activity.
- Run endpoint detection and response (EDR) in block mode so that Microsoft Defender for Endpoint can block malicious artifacts, even when your non-Microsoft antivirus does not detect the threat or when Microsoft Defender Antivirus is running in passive mode. EDR in block mode works behind the scenes to remediate malicious artifacts that are detected post-breach.
- Enable investigation and remediation in full automated mode to allow Microsoft Defender for Endpoint to take immediate action on alerts to resolve breaches, significantly reducing alert volume.
- Turn on block mode in Microsoft Defender Antivirus, or the equivalent for your antivirus product, to cover rapidly evolving attacker tools and techniques. Cloud-based machine learning protections block a majority of new and unknown variants.
- Microsoft Defender customers can turn on attack surface reduction rules to prevent common attack techniques used in ransomware attacks. Attack surface reduction rules are sweeping settings that are effective at stopping entire classes of threats:
    - Block executable files from running unless they meet a prevalence, age, or trusted list criterion
    - Use advanced protection against ransomware
    - Block web shell creation for servers

Microsoft Defender XDR detections

Following the release of the vulnerability, the Microsoft Defender Research Team ensured that protections are deployed for customers, from ensuring that Microsoft Defender Vulnerability Management correctly identifies and surfaces all vulnerable devices in impacted customer environments, to building Microsoft Defender for Endpoint detections and alerting along the attack chain.

Microsoft Defender Vulnerability Management customers can search for this vulnerability in the Defender Portal or navigate directly to the CVE page to view a detailed list of the exposed devices within their organization.

Customers of Microsoft Defender Experts for XDR that might have been impacted have also been notified of any post-exploitation activity and recommended actions.

Microsoft Defender XDR customers can refer to the list of applicable detections below. Microsoft Defender XDR coordinates detection, prevention, investigation, and response across endpoints, identities, email, apps to provide integrated protection against attacks like the threat discussed in this blog.

Customers with provisioned access can also use Microsoft Security Copilot in Microsoft Defender to investigate and respond to incidents, hunt for threats, and protect their organization with relevant threat intelligence.

Tactic	Observed activity	Microsoft Defender coverage
Initial access	Exploitation of GoAnywhere MFT via deserialization in	**Microsoft Defender for Endpoint** detects possible exploitation via the

	Licensing Service	following alert: – Possible exploitation of GoAnywhere MFT vulnerability **Microsoft Defender Experts for XDR** can detect possible exploitation via the following alerts: – Possible exploitation of vulnerability in GoAnywhere Tomcat – Possible discovery activity following successful Tomcat vulnerability exploitation **Microsoft Defender Vulnerability Management(MDVM)** surfaces devices vulnerable to CVE-2025-10035. **Microsoft Defender External Attack Surface Management** Attack Surface Insights with the following title can indicate vulnerable devices on your network but is not necessarily indicative of exploitation: – [Potential] CVE-2025-10035 – GoAnywhere MFT Command Injection via Deserialization in Licensing Service (**Note**: An Attack Surface Insight marked as potential indicates a service is running but cannot validate whether that service is running a vulnerable version. Check resources to verify that they are up to date.)
Persistence	Dropping and abuse of remote monitoring and management (RMM) tool and suspected web shell deployment; creation of *.jsp* files within the GoAnywhere MFT directories	**Microsoft Defender for Endpoint** detects possible signs of the attacker deploying persistence mechanisms via the following alerts: – Uncommon remote access software – Remote access software – Suspicious file dropped and launched – Suspicious service launched – Suspicious account creation – User account created under suspicious circumstances – New local admin added using Net commands – New group added suspiciously – Suspicious Windows account manipulation – Ransomware-linked threat actor detected
Discovery	User and system discovery commands; deployment of	**Microsoft Defender for Endpoint** detects malicious exploration

	tools such as netscan for network discovery	activities via the following alerts: – Suspicious sequence of exploration activities – Anomalous account lookups – Suspicious Windows account manipulation
Command and control	Use of RMM tools for establishing C2 infrastructure and setup of Cloudflare tunnel for secure C2 communication	**Microsoft Defender for Endpoint** detects C2 activities observed in this campaign via the following alerts: – Uncommon remote access software – Remote access software
Exfiltration	Rclone deployment and execution	**Microsoft Defender for Endpoint** detects exfiltration activities observed in this campaign via the following alert: – Ransomware-linked threat actor detected
Actions on objectives	Deployment of Medusa ransomware	**Microsoft Defender Antivirus** detects the ransomware payload used in this attack as the following threat: – Ransom:Win32/Medusa **Microsoft Defender for Endpoint** detects the ransomware payload via the following alerts: – Ransomware-linked threat actor detected

Microsoft Security Copilot

Security Copilot customers can use the standalone experience to create their own prompts or run the following prebuilt promptbooks to automate incident response or investigation tasks related to this threat:

- Incident investigation
- Microsoft User analysis
- Threat actor profile
- Threat Intelligence 360 report based on MDTI article
- Vulnerability impact assessment

Note that some promptbooks require access to plugins for Microsoft products such as Microsoft Defender XDR or Microsoft Sentinel.

Threat intelligence reports

Microsoft Defender XDR customers can use the following threat analytics reports in the Defender portal (requires license for at least one Defender XDR product) to get the most up-to-date information about the threat actor, malicious activity, and techniques discussed in this blog. These reports provide the intelligence,

protection information, and recommended actions to prevent, mitigate, or respond to associated threats found in customer environments.

Microsoft Defender XDR threat analytics

- Vulnerability profile: CVE-2025-10035 – GoAnywhere Managed File Transfer
- Actor profile: Storm-1175

Microsoft Security Copilot customers can also use the Microsoft Security Copilot integration in Microsoft Defender Threat Intelligence, either in the Security Copilot standalone portal or in the embedded experience in the Microsoft Defender portal to get more information about this threat actor.

Hunting queries

Microsoft Defender XDR

Microsoft Defender XDR customers can run the following query to find related activity in their networks:

Vulnerable devices

Find devices affected by the CVE-2025-10035 vulnerability.

```
DeviceTvmSoftwareVulnerabilities
| where CveId in ("CVE-2025-10035")
| summarize by DeviceName, CveId
```

Possible GoAnywhere MFT exploitation

Look for suspicious PowerShell commands indicative of GoAnywhere MFT exploitation. These commands are also detected with the Defender for Endpoint alert *Possible exploitation of GoAnywhere MFT vulnerability*.

```
DeviceProcessEvents
| where InitiatingProcessFolderPath contains @"\GoAnywhere\"
| where InitiatingProcessFileName contains "tomcat"
| where InitiatingProcessCommandLine endswith "//RS//GoAnywhere"
| where FileName == "powershell.exe"
| where ProcessCommandLine has_any ("whoami", "systeminfo", "net user", "net group",
"localgroup administrators", "nltest /trusted_domains", "dsquery", "samaccountname=", "query
session", "adscredentials", "o365accountconfiguration", "Invoke-Expression",
"DownloadString", "DownloadFile", "FromBase64String",  "System.IO.Compression",
"System.IO.MemoryStream", "iex ", "iex(", "Invoke-WebRequest", "set-MpPreference", "add-
MpPreference", "certutil", "bitsadmin")
```

Look for suspicious cmd.exe commands launched after possible GoAnywhere MFT exploitation. These commands are also detected with the Defender for Endpoint alert *Possible exploitation of GoAnywhere MFT vulnerability*.

```
DeviceProcessEvents
| where InitiatingProcessFolderPath contains @"\GoAnywhere\"
| where InitiatingProcessFileName contains "tomcat"
```

```
| where InitiatingProcessCommandLine endswith "//RS//GoAnywhere"
| where ProcessCommandLine !contains @"\GIT\"
| where FileName == "cmd.exe"
| where ProcessCommandLine has_any ("powershell.exe", "powershell ", "rundll32.exe",
"rundll32 ", "bitsadmin.exe", "bitsadmin ", "wget http", "quser") or ProcessCommandLine
has_all ("nltest", "/dclist") or ProcessCommandLine has_all ("nltest", "/domain_trusts") or
ProcessCommandLine has_all ("net", "user ", "/add") or ProcessCommandLine has_all ("net",
"user ", " /domain") or ProcessCommandLine has_all ("net", " group", "/domain")
```

Storm-1175 indicators of compromise

The following query identifies known post-compromise tools leveraged in recent GoAnywhere exploitation activity attributed to Storm-1175. Note that the alert *Ransomware-linked threat actor detected* will detect these hashes.

```
let fileHashes =
dynamic(["4106c35ff46bb6f2f4a42d63a2b8a619f1e1df72414122ddf6fd1b1a644b3220",
"c7e2632702d0e22598b90ea226d3cde4830455d9232bd8b33ebcb13827e99bc3",
"cd5aa589873d777c6e919c4438afe8bceccad6bbe57739e2ccb70b39aee1e8b3",
"5ba7de7d5115789b952d9b1c6cff440c9128f438de933ff9044a68fff8496d19"]);
union
(
DeviceFileEvents
| where SHA256 in (fileHashes)
| project Timestamp, FileHash = SHA256, SourceTable = "DeviceFileEvents"
),
(
DeviceEvents
| where SHA256 in (fileHashes)
| project Timestamp, FileHash = SHA256, SourceTable = "DeviceEvents"
),
(
DeviceImageLoadEvents
| where SHA256 in (fileHashes)
| project Timestamp, FileHash = SHA256, SourceTable = "DeviceImageLoadEvents"
),
(
DeviceProcessEvents
| where SHA256 in (fileHashes)
| project Timestamp, FileHash = SHA256, SourceTable = "DeviceProcessEvents"
)
| order by Timestamp desc
```

Indicators of compromise

File IoCs (RMM tools in identified Storm-1175 exploitation activity):

- 4106c35ff46bb6f2f4a42d63a2b8a619f1e1df72414122ddf6fd1b1a644b3220 (MeshAgent SHA-256)
- c7e2632702d0e22598b90ea226d3cde4830455d9232bd8b33ebcb13827e99bc3 (SimpleHelp SHA-256)
- cd5aa589873d777c6e919c4438afe8bceccad6bbe57739e2ccb70b39aee1e8b3 (SimpleHelp SHA-256)
- 5ba7de7d5115789b952d9b1c6cff440c9128f438de933ff9044a68fff8496d19 (SimpleHelp SHA-256)

Network IoCs (IPs associated with SimpleHelp):

- 31[.]220[.]45[.]120
- 45[.]11[.]183[.]123
- 213[.]183[.]63[.]41

References

Learn more

For the latest security research from the Microsoft Threat Intelligence community, check out the Microsoft Threat Intelligence Blog.

To get notified about new publications and to join discussions on social media, follow us on LinkedIn, X (formerly Twitter), and Bluesky.

To hear stories and insights from the Microsoft Threat Intelligence community about the ever-evolving threat landscape, listen to the Microsoft Threat Intelligence podcast.