To: Gateway Technical College Cybersecurity Major Students
From: Benjamin Bell
Subject: Notice on CVE-2025-21298
Date: March 6, 2025

Summary:
In December 2025, the Mitre Corporation announced a new Common Vulnerability and Exploit (CVE) labelled CVE-2025-21298 (Mitre, 2025). The Vulnerability is rated as a 9.8 out of 10 on the Common Vulnerability Scoring System, a scale that cybersecurity professionals use as a scoring mechanism to rate the potential danger that malware poses to computer systems. This malware targets Windows Object Linking and Embedding (OLE) technology on Windows systems. Upon successful exploitation, an attacker is able to execute remote code execution which means that they can execute code used to take over a person's machine despite being across the globe.

Purpose:
The purpose of this writing is to inform and equip users of the Windows vulnerability and the knowledge to effectively mitigate it. Successful exploitation of this vulnerability presents extreme consequences including but not limited to, privilege escalation and root access.

Introduction:
CVE-2025-21298 is classified as a Remote Code Execution Vulnerability that affects Windows Systems (Offsec, 2025). The vulnerability is exploited when an attacker embeds malicious code to a text document that allows embedded elements like Rich Text Format files using Windows Object Linking and Embedding (OLE) technology. These Rich Text Format files allow file embedding and are used as text documents that can be shared and processed by many different word processors (Adobe, 2025). The attacker can then attach the document to an email and send it to the victim host. When a host uses email software like Microsoft Outlook, the email is previewed automatically due to a feature that is enabled by default and the malicious code is executed without user interaction.

Causes and Effect:
The causes of the vulnerability stem from the OLE technology that allows the embedding of malicious code to files. Without proper input validation of the strings that are embedded, there is no limit to the code that can be embedded to files. Another cause of the vulnerability is the automatic preview of emails and files that is enabled on Outlook. This feature is disabled by default at the time of writing but there are many users who enable and frequently use the feature. Without the proper security measures in place to filter senders and their content, users are sitting ducks waiting to be exploited. After they are exploited, the effects are potentially disastrous. With remote code execution in an active exploit, a malicious actor has unlimited remote control

over a host machine. This presents risks in data privacy, denial of service, and privilege escalation. With elevated privileges, an attacker can traverse the network to expand the magnitude of their attack by gaining access to resources only available to administrators. In order to mitigate the vulnerability, Microsoft recommends viewing emails in plaintext (Microsoft, 2025). It should also be noted that proper security measures should be in place for identity and access management to prevent privilege escalation if a host in the organization network is compromised. It is also suggested to disable the preview feature on Microsoft Outlook and/or checking to see if the email provider has a similar feature that may make the user vulnerable. Lastly, make sure to update devices frequently to stay up to date with the latest bug fixes and security updates that the manufacturer puts out. These updates fix code issues that allow the vulnerabilities to occur.

To better understand the impact and magnitude of this vulnerability in a high stakes setting, Staff Sergeant, Intelligence Analyst in the United States Army gave input.

Q: How has this vulnerability affected you in such a high stakes role?
A: “Despite not having direct contact with this specific vulnerability, it’s important for my soldiers and myself to be aware of threats like this that can threaten our computer systems and threaten national security.”

Q: What does this vulnerability mean for nation state actors and our own intelligence force?
A: “I think it’s critical for us to know about threats that can pose a risk of this magnitude. If adversaries can use these vulnerabilities to exploit our systems, we can see a lot of bad things happen to our country. It’s always important for our military intelligence to stay up to date on the most current threat.”

Q: How will other vulnerabilities like this once affect the military going forward?
A: “We will always have to stay on our toes and stay ahead of our adversaries. Intelligence is all about what you know. That intelligence serves as the deciding factor between mission success and failure. “

Conclusion:
With a CVSS score of 9.8, it is safe to say that exploitation of this vulnerability on a host device in the network would present significant issues and challenges. It is important for professionals in our field to stay up to date on the latest vulnerabilities to best protect ourselves and our clients. Make sure to take the proper measures to protect the network and spread the knowledge of these vulnerabilities to fellow colleagues and others at risk. The intelligence of the threat and remediation methods can serve as the difference between life as we know it and severe repercussions.

Works Cited:

Team, OffSec. “CVE-2025-21298: A Critical Windows Ole Zero-Click Vulnerability.” *OffSec*, 4 Feb. 2025, www.offsec.com/blog/cve-2025-21298/.

“Windows OLE Remote Code Execution Vulnerability.” *Security Update Guide - Microsoft Security Response Center*, 14 Jan. 2025, msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21298.

“RTF File Format: What Is Rich Text Format? | Adobe Acrobat.” *What Is Rich Text Format and What Is It Used For?*, Adobe, www.adobe.com/acrobat/hub/what-is-rich-text-format.html. Accessed 6 Mar. 2025.

“CVE-2025-21298.” *CVE*, MITRE, 10 Dec. 2024, cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2025-21298.

Interview:

SSG, Intelligence Analyst. Military Unit, North Carolina (Personal Communication, Feb 24, 2025) phone: XXX-XXX-XXXX