AL2025_48 Microsoft Outlook Stops Displaying Inline SVG Images Exploited in Phishing Attacks (October 07th , 2025)

Description

Microsoft has implemented a security change in Outlook to block the display of inline SVG (Scalable Vector Graphics) images, following recent phishing campaigns that weaponized SVG content to deliver malicious payloads. Attackers embedded harmful scripts and links within SVG files attached to or displayed in Outlook messages, tricking recipients into interacting with them. This technique bypassed traditional attachment filters and was used to distribute credential-stealing malware through deceptive email messages.

The update applies to Outlook desktop, web, and mobile clients, ensuring that inline SVG images are no longer automatically rendered in email messages. Instead, users will see a placeholder icon or broken image symbol where the SVG would normally appear. The change aims to prevent drive-by phishing attempts and the execution of malicious embedded content.

Attack Details

In recent phishing campaigns, attackers leveraged SVG images to disguise malicious redirects or encoded scripts inside visually appealing email graphics. Once clicked, users were redirected to fake login pages or had malicious code executed via embedded links. These attacks exploited the ability of SVG files to contain JavaScript and HTML elements. By stopping the inline display of SVG files, Microsoft disrupts this attack vector, preventing users from unknowingly interacting with malicious embedded content. Outlook users can still receive SVG attachments but must download them manually for viewing, reducing the risk of automatic exploitation.

Remediation

- **Ensure Outlook is Updated:** Apply the latest Microsoft Outlook security updates to enable the SVG display restriction.
- **User Awareness:** Educate staff on phishing techniques leveraging image-based lures and encourage caution when opening unexpected attachments or email content.
- **Attachment Filtering:** Configure mail gateways to quarantine or block suspicious image attachments (e.g., SVG, HTML) from external senders.
- **Use Advanced Threat Protection:** Enable Microsoft Defender or similar security tools to scan and isolate malicious attachments.
- **Review Email Policies:** Disable automatic image downloads and restrict active content in emails.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

- Gatlan, S. (2025, October 3). Microsoft Outlook stops displaying inline SVG images used in attacks. BleepingComputer. Retrieved from https://www.bleepingcomputer.com/news/security/microsoft-outlook-stops-displaying-inline-svg-images-used-in-attacks/

- Bitdefender. (2025, October 3). Microsoft Outlook blocks inline SVG images to curb security threats. Bitdefender HotforSecurity. Retrieved from https://www.bitdefender.com/en-us/blog/hotforsecurity/microsoft-outlook-blocks-inline-svg-images-to-curb-security-threats