# AL2024_30 New Windows SmartScreen Zero-Day Exploit (August 15th , 2024)

## Description

On August 13, 2024, Microsoft disclosed a critical security vulnerability (CVE-2024-38213) in Windows SmartScreen that has been actively exploited as a zero-day since March 2024. SmartScreen, a security feature introduced with Windows 8, is designed to protect users from malicious software by marking downloaded files with a Mark of the Web (MotW) label. However, attackers have found a way to bypass this protection, allowing them to execute malicious payloads without triggering security warnings.

## Attack Details

The vulnerability, CVE-2024-38213, is a remote, unauthenticated exploit that requires user interaction, making it more challenging for threat actors to successfully carry out attacks. However, once exploited, this vulnerability allows attackers to bypass the SmartScreen user experience, effectively rendering the security feature useless.

The attackers employed a technique they named "copy2pwn," where files from a WebDAV share were copied locally without triggering the MotW protections. This bypass enabled the execution of malicious payloads disguised as legitimate software installers, including those for Apple iTunes, Notion, and NVIDIA.

## Remediation

To mitigate the risk associated with CVE-2024-38063, Microsoft recommends several actions:

1. **Apply Patches Promptly:** Regularly update systems with the latest security patches from Microsoft to mitigate known vulnerabilities.
2. **Limit User Interaction with Unknown Files:** Educate users about the dangers of opening files from untrusted sources.
3. **Monitor Network Traffic:** Implement network monitoring to detect unusual activity related to WebDAV shares or other remote file access that could indicate an ongoing attack.

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

## References

Gatlan, S. (2024, August 15). New Windows SmartScreen bypass exploited as zero-day since March. Retrieved from BleepingComputer. https://www.bleepingcomputer.com/news/microsoft/new-windows-smartscreen-bypass-exploited-as-zero-day-since-march/

Girnus, P. (2024, August 15). Zero Day Initiative CVE-2024-38213: Copy2PWN Exploit EVades Windows Web Protections. Retrieved fromZero Day Initiative. https://www.zerodayinitiative.com/blog/2024/8/14/cve-2024-38213-copy2pwn-exploit-evades-windows-web-protections