مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

# Windows Kernel Vulnerability Exploited in Active Attacks

Tracking #:432316640

Date:17-12-2024



TLP: WHITE

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity Windows kernel vulnerability (CVE-2024-35250) is currently being exploited in the wild.

## TECHNICAL DETAILS:

A high-severity Windows kernel vulnerability (CVE-2024-35250) is currently being exploited in the wild. This vulnerability, discovered by the DEVCORE Research Team and reported through Trend Micro's Zero Day Initiative, allows local attackers to escalate privileges and gain SYSTEM privileges on vulnerable systems. This flaw, related to untrusted pointer dereferencing in the Microsoft Kernel Streaming Service (MSKSSRV.SYS), has been successfully exploited in low-complexity attacks that do not require user interaction. Despite being patched by Microsoft in June 2024, exploit code for this vulnerability has been publicly released, increasing the risk of exploitation.

**Vulnerability Overview:**

- Vulnerability Type: Untrusted Pointer Dereference (Privilege Escalation)
- Affected Component: Microsoft Kernel Streaming Service (MSKSSRV.SYS)
- Exploitation Complexity: Low (No user interaction required)
- Exploitable On: Windows 11 (and potentially other supported Windows versions)
- Proof of Concept (PoC): A proof-of-concept exploit for this vulnerability was publicly released on GitHub four months after Microsoft's initial patch in June 2024.

## RECOMMENDATIONS:

- Patch Immediately: Ensure that all Windows systems, especially those running Windows 11 or other vulnerable versions, are updated with the latest patches. Microsoft patched this vulnerability in June 2024, so systems should be checked to confirm that they are up-to-date.
- Monitor for Exploitation: Since a proof-of-concept exploit is publicly available, it is highly recommended to actively monitor for signs of exploitation on affected systems.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

## REFERENCES:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-35250