Alert Bulletin

Bulletin N.: 2024-34
Publication Date: 17/09/2024
Subject: Alert 2024-34 Public POC for CVE-2024-38080 in Hyper-V
Traffic Light Protocol (TLP): White

Affected Product(s):

Windows Hyper-V

Description:

In July, the vulnerability CVE-2024-38080 (CVSS 7.8) was disclosed, which affects Windows Hyper-V, Microsoft's hypervisor used for virtualized environments. This is a privilege escalation (EoP) vulnerability that has already been exploited in the wild and is listed in CISA's Known Exploited Vulnerabilities Catalog.

The flaw lies in the VidExoBrokerIoctlReceive function of Hyper-V and stems from an integer overflow, allowing malicious actors to manipulate system memory. By exploiting this vulnerability, attackers can execute code with SYSTEM-level privileges, achieving full control of the compromised system.

Recently, a security researcher published a detailed analysis and proof-of-concept (PoC) code for this critical vulnerability, which has already been patched in Windows Hyper-V. However, the vulnerability poses a significant risk for organizations that rely on Microsoft's virtualization.

The PoC for this vulnerability is publicly available on GitHub, increasing the risk for organizations using Hyper-V for critical workloads, as it provides a clear guide for attackers to replicate the exploit. As a result, it is likely to be actively exploited in the near future.