Windows Hyper-V research.

Quadron attaches great importance to researching zero-day vulnerabilities in modern softwares, Operation Systems, IoT devices and web applications. Our research covers several areas. Paying special attention to researching kernel-level vulnerabilities in operating systems and examining IoT devices. Our current main area of research is Microsoft Hyper-V. Hyper-V is an extremely complex application ..... Nevertheless, our research so far is fruitful, we found bug in three virtualization drivers that could cause the system to crash.

A denial of service vulnerability exists when Windows improperly handles objects in memory. An attacker who successfully exploited the vulnerability could cause a target system to stop responding.

To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application or to convince a user to open a specific file on a network share. The vulnerability would not allow an attacker to execute code or to elevate user rights directly, but it could be used to cause a target system to stop responding.

The Proof of Concept codes that cause the error can be found in the Quadron Research Lab's github repository.

https://github.com/Quadron-Research-Lab/Kernel_Driver_bugs/tree/main/Hyper-V_VfpExt

https://github.com/Quadron-Research-Lab/Kernel_Driver_bugs/tree/main/Hyper-V_VmSwitch.sys_NDIS

https://github.com/Quadron-Research-Lab/Kernel_Driver_bugs/tree/main/Hyper-V_Synth3dVsp