MECHREVO Control Console Has Privilege Escalation Vulnerability

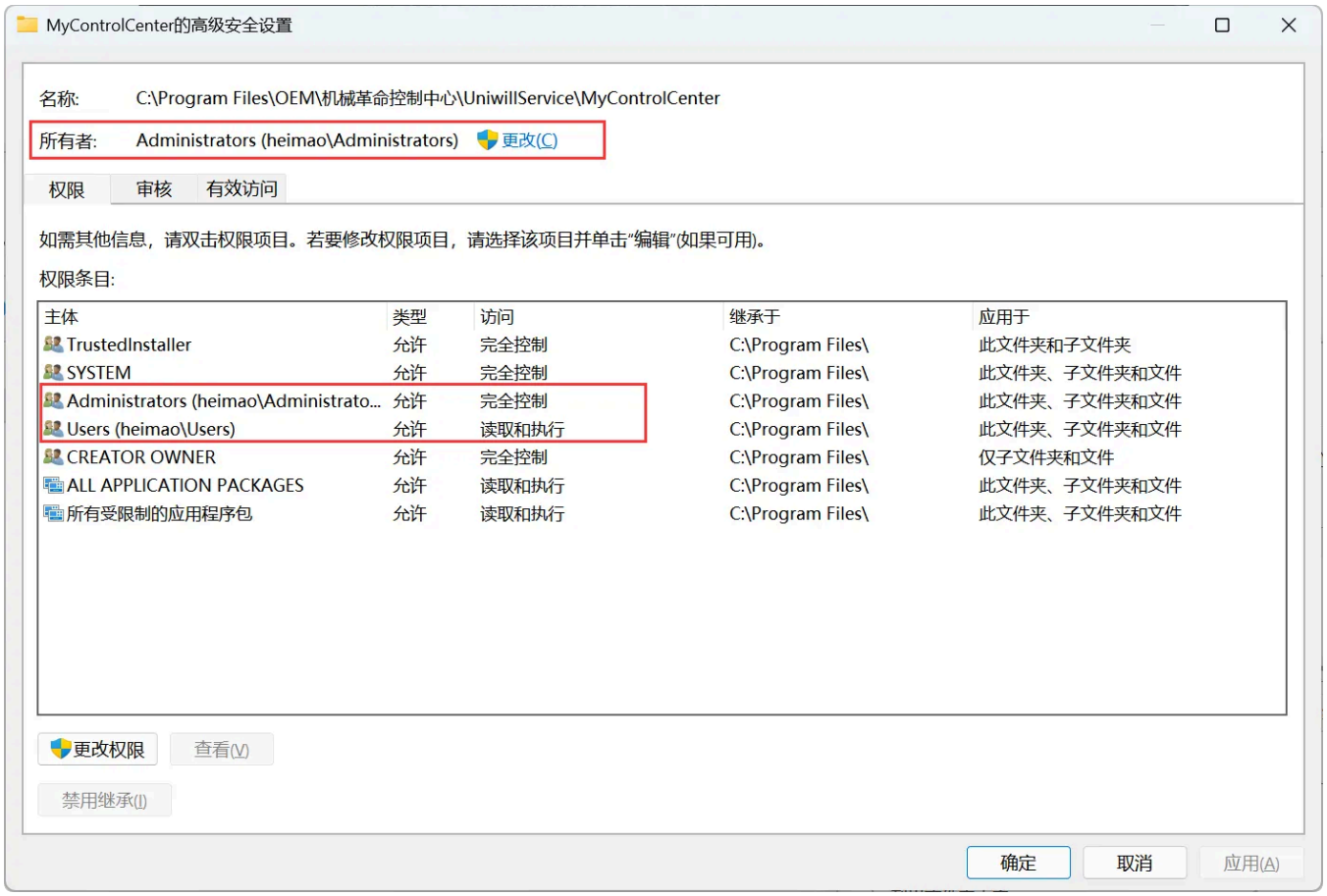
MECHREVO is a Chinese gaming laptop brand primarily focused on high-performance gaming laptops, ultrabooks, and design laptops. Brand background: Founded in 2014, it is a collaboration between Tsinghua Tongfang and MSI, leveraging Tongfang's supply chain and MSI's gaming laptop technology. Positioning: It offers cost-effective gaming laptops, competing with brands like Lenovo Legion and ASUS ROG, often at more competitive prices.

Official website: https://www.mechrevo.com/#anchor2 <https://www.mechrevo.com/#anchor2>

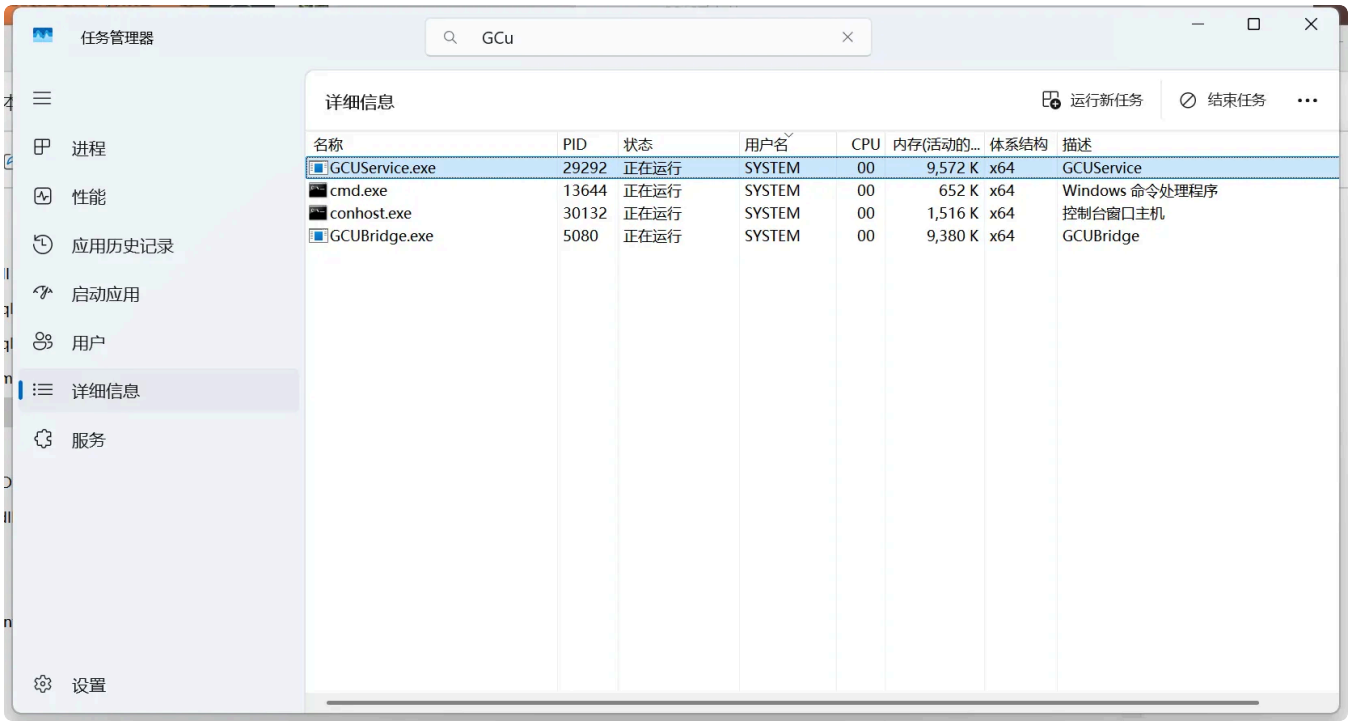
MECHREVO-branded computers come with a pre-installed control console located in the following directory:

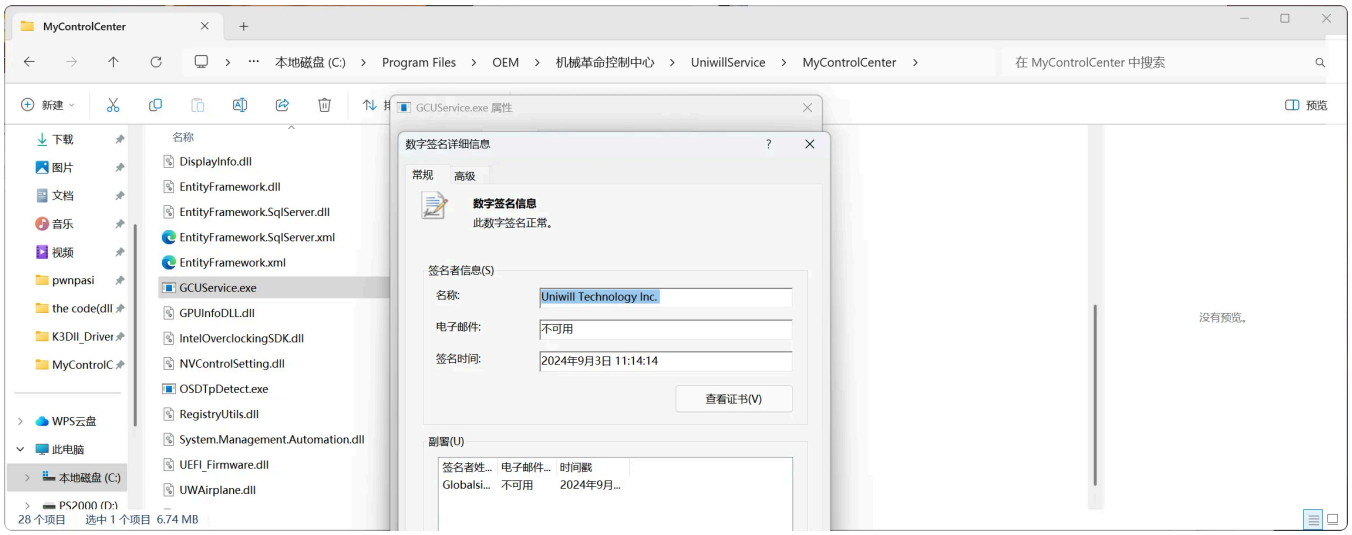
```
C:\Program Files\OEM\机械革命控制中心\UniwillService\MyControlCenter
```

User accounts can access this folder, while administrators have full permissions over it.

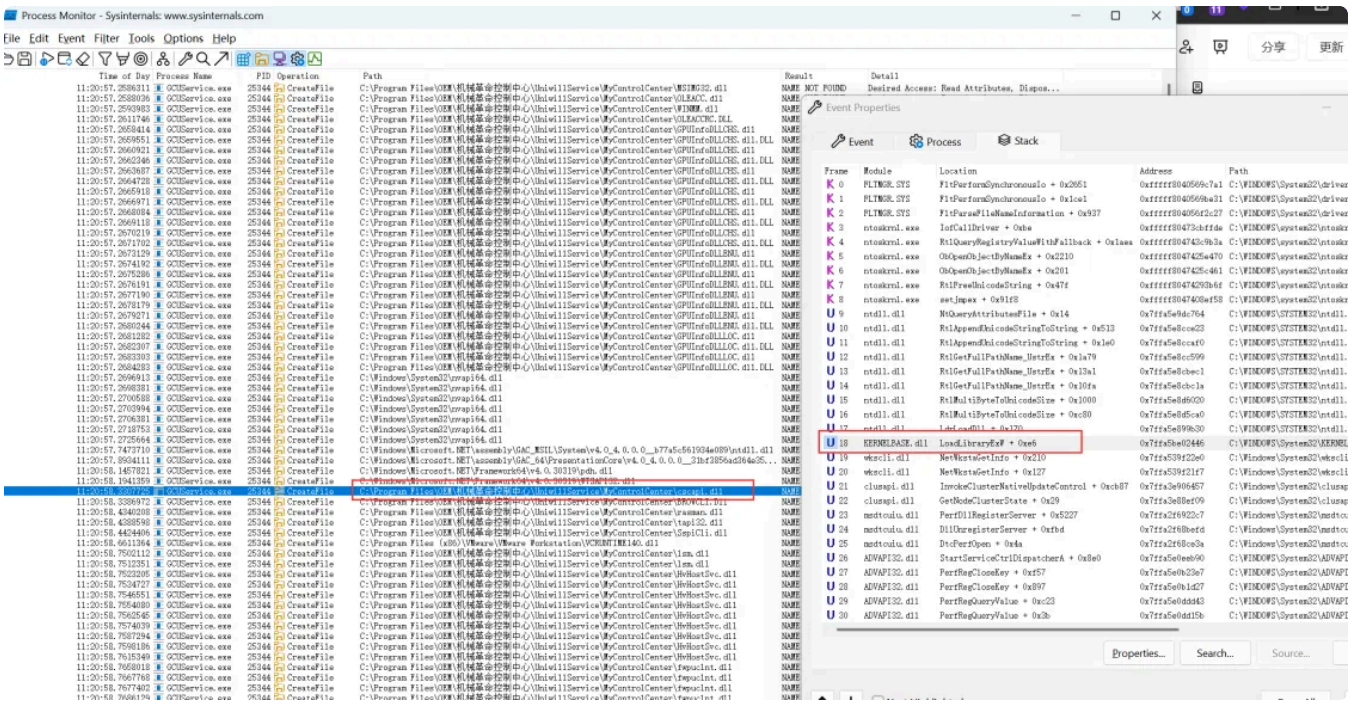


When the control console runs, it starts a console service with SYSTEM privileges, and it automatically restarts every 5 seconds.

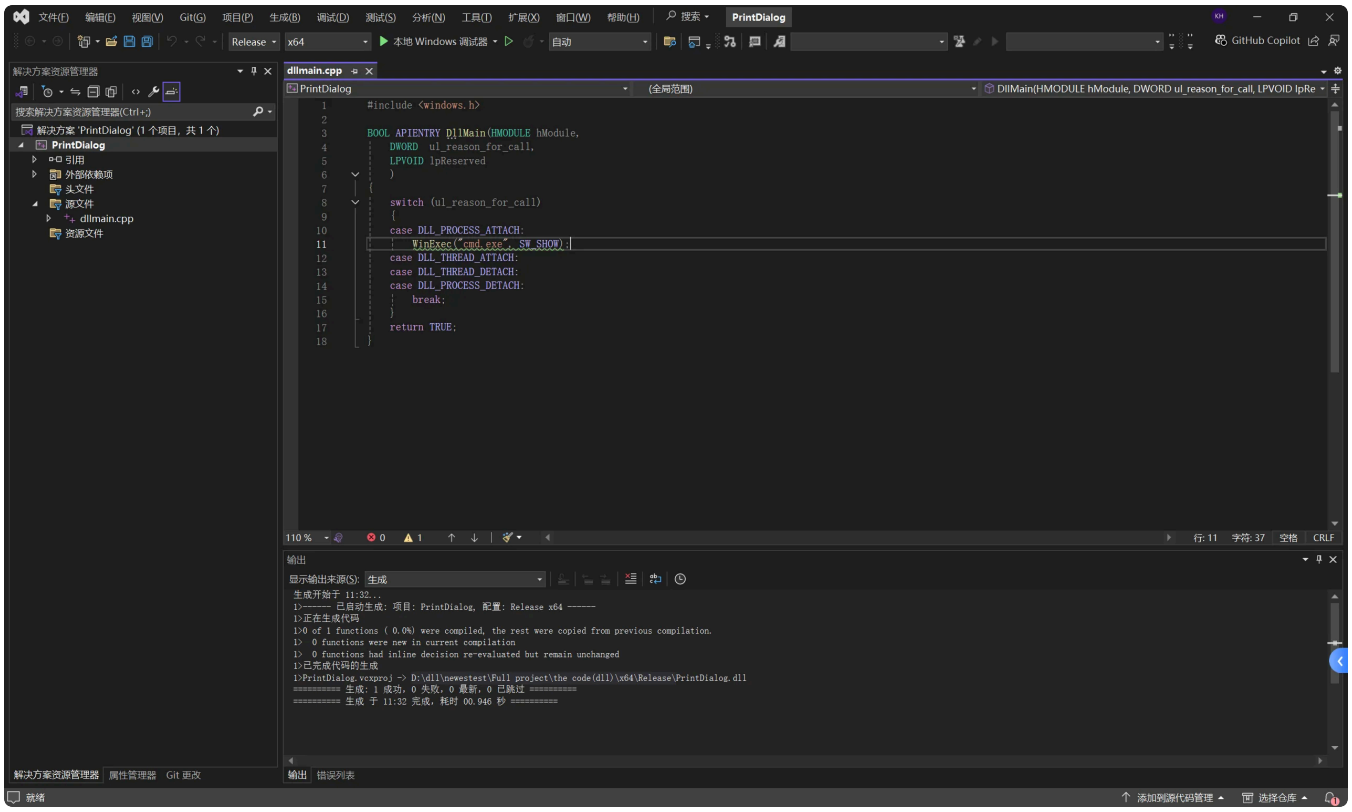




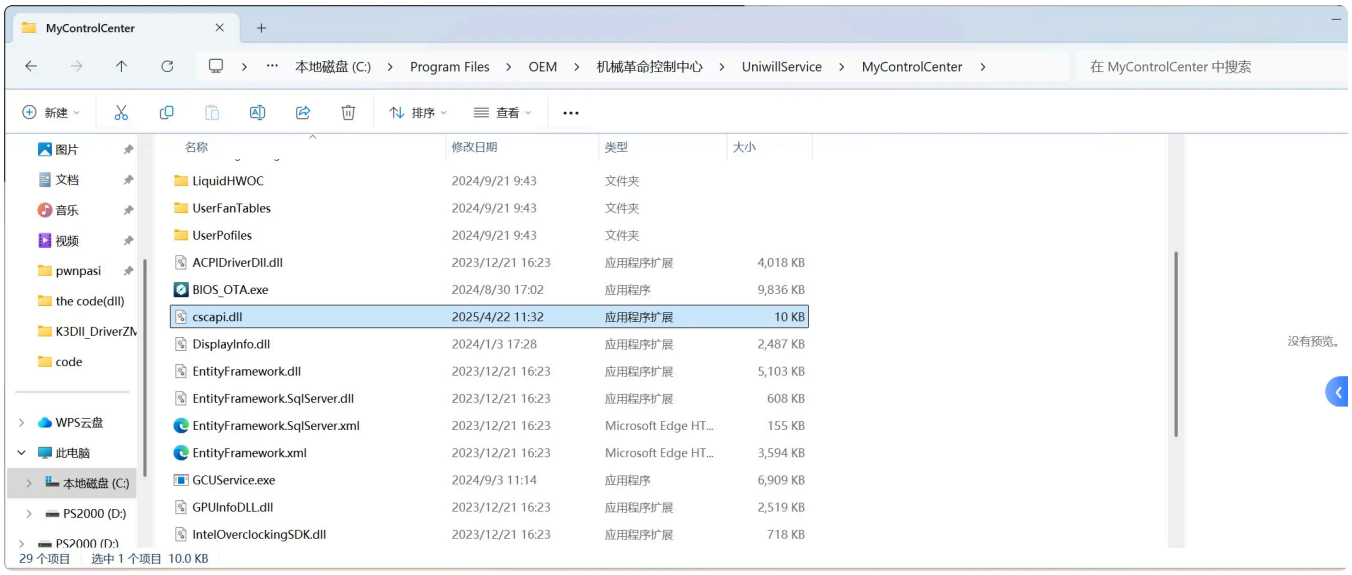
When the control console runs, it loads a file named `cscapi.dll` from the current directory into the stack and executes it. A malicious `cscapi.dll` can be placed in the `GCUService.exe` directory to exploit this vulnerability for privilege escalation.



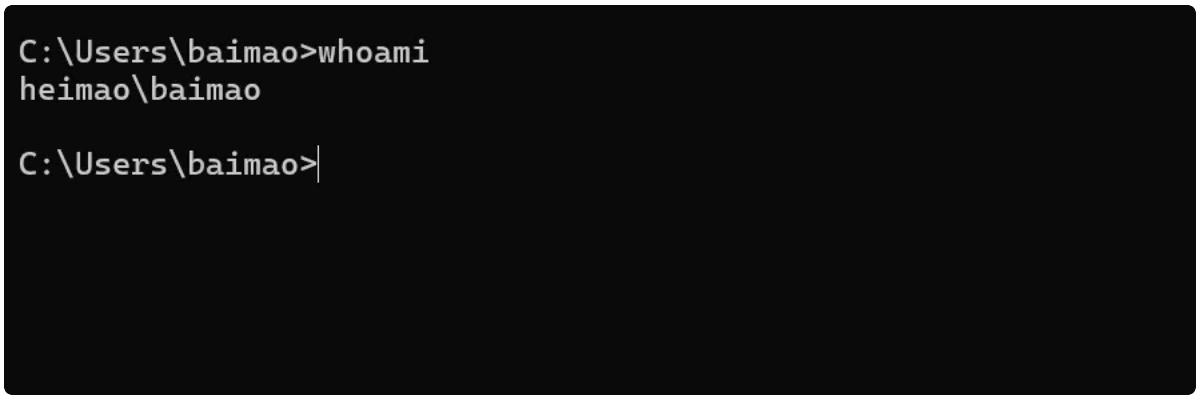
Verification: A `cscapi.dll` was generated to launch `cmd.exe`.

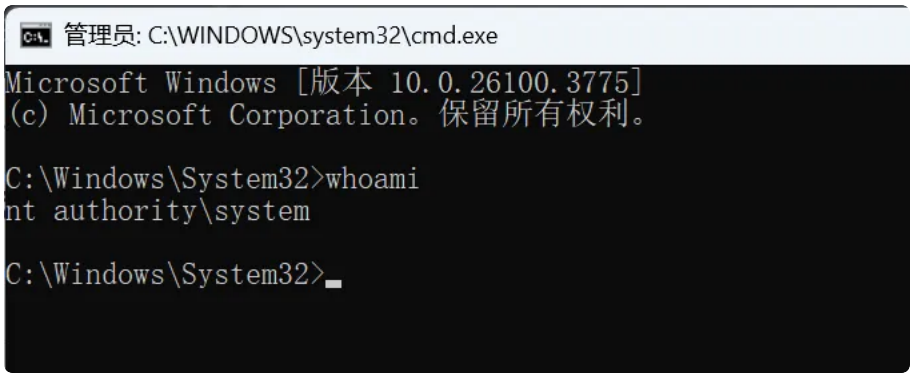


The DLL was placed in the `C:\Program Files\OEM\MECHREVO Control Center\Uniwill Service\MyControlCenter` directory. There was no need to stop the service, as it restarts every 5 seconds.



Successful privilege escalation from user-level to SYSTEM-level was achieved.





The most important thing about this vulnerability is that you don't need to stop the service, it will automatically start every five seconds. Therefore, you only need to put the malicious DLL into a folder. The difficulty of exploitation is very low, but the harm is high

video：

Note

The vendor was contacted early about this disclosure but did not respond in any way.