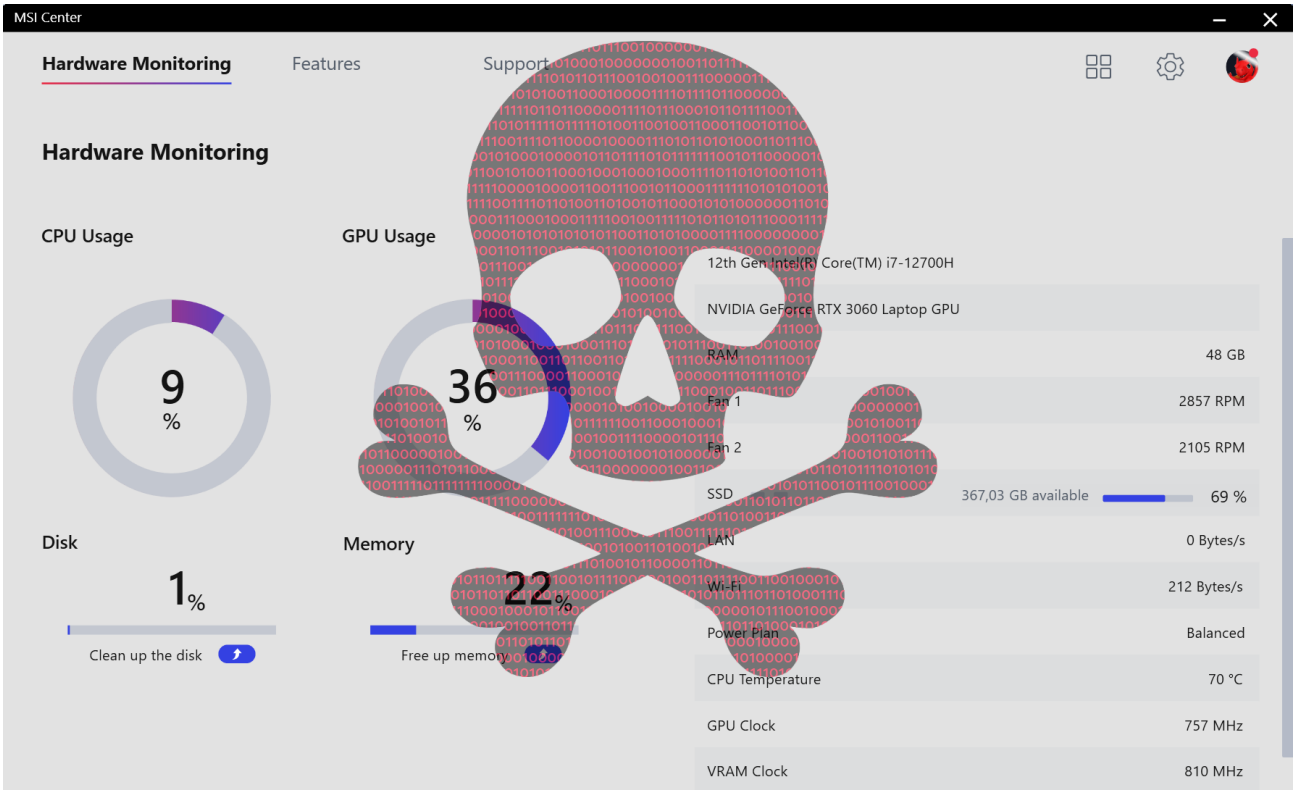
README.md

Local privilege escalation in MSI Center desktop application.



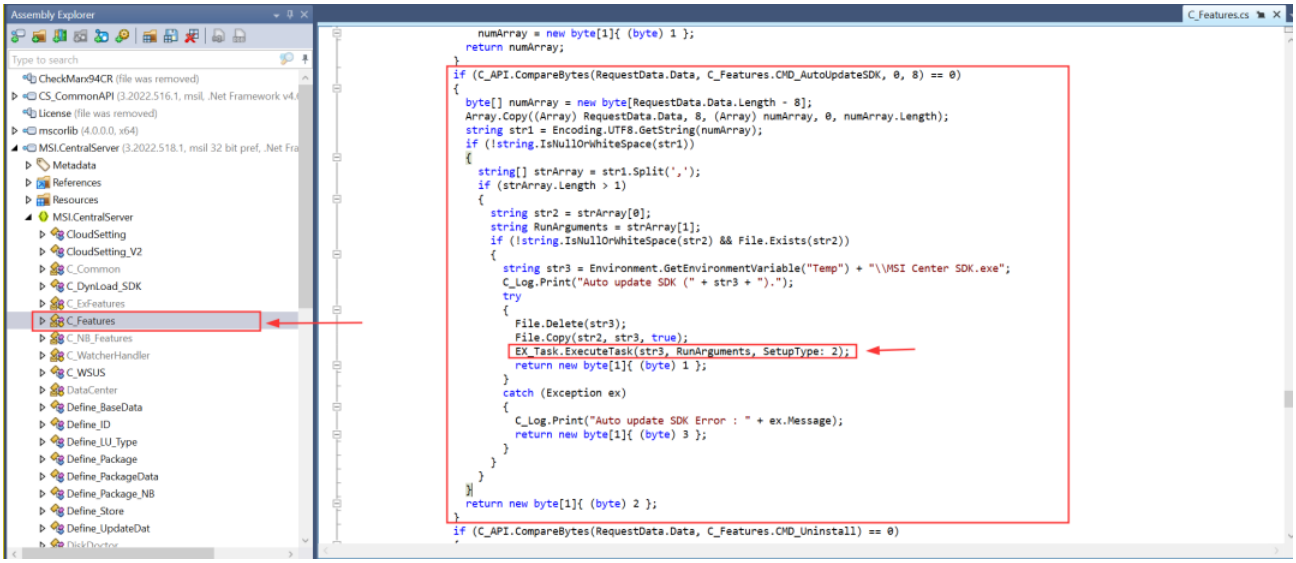
The vulnerability exist in "C_Features" of MSI.CentralServer.exe. MSI.CentralServer.exe is an application that gathers information about your system, it collaborates with MSI.TerminalServer.exe. The ExecuteTask function which we can call it in "CMD_AutoUpdateSDK" gives us a chance to run an exectable with custom parameters under Administrative privileges. You can see the related port only from localhost.

```
PS C:\Windows\system32> Get-Process -Id (Get-NetTCPConnection -LocalPort 32682).OwningProcess

Handles  NPM(K)    PM(K)      WS(K)     CPU(s)      Id  SI ProcessName
-------  ------    -----      -----     ------      --  -- -----------
      0       0       60          8                0   0 Idle
    914      52    38740      61660       1,89  13848   4 MSI.CentralServer
```

The vulnerability

You can easily disassemble the MSI.CentralServer.exe using any .NET disassembler. Central Server itself listens on 32682 port from localhost, we can find the source code of the handler in "C_Features". Just look at the CMD_AutoUpdateSDK feature to see the vulnerability. We abuse this feature (it is automatic updater of MSI Center). It receives the user-given payload, splits it into multiple parts to execute the command with custom parameters.



This is main function which our feature uses it to execute given PE with custom arguments:

```
public static int ExecuteTask(
  string RunExePath,
  string RunArguments,
  bool IsSupervisor = true,
  int SetupType = 0)
{
  return EX_Task.ExecuteTask(RunExePath, RunArguments, "", IsSupervisor, SetupType);
}
```

The port which MSI Central Server listens is updated in 1.0.59.0 version. It is 32683.

POC

You can generate your own payload, hex it and run the script in the local computer. The POC creates hacker user with "hacker123" password and adds it to the Administrators group.

Proof-of-Concept video: https://user-images.githubusercontent.com/64528432/188067866-f30fe089-db76-4cc0-81ce-f74871769b33.mp4

Languages

- **Python** 100.0%