Find a vulnerability that causes Windows computers to have a 'white screen of death' error

CyberArk security researcher Eviatar Gerzi has found serious DoS (denial of service) vulnerabilities in Windows terminals and Chrome web browsers.

Recently, Eviatar Gerzi has been researching attack methods based on the old story in 2003 that it is possible to execute code through editing the window title. Finally, he discovered that it was possible to attack by quickly changing the window title on PuTTY.

This type of attack causes Gerzi's test machine to enter a state known as the "white screen of death (WSOD)". In that state, everything freezes except the mouse pointer.

When trying the same attack on a local application, the system immediately fell into WSOD because the core of the operating system was overloaded by the calls.

The misused function is called "SetWindowsText", which allows to convert the text of the title bar of the specified window.

The only way to get out of the WSOD state is to restart the computer. Therefore, this attack can be used to generate DoS states across a wide range of applications.

Not only "SetWindowsText" is an abused function, though. With the MobaXterm terminal, the function that is abused to cause an error is GdipDrawString. However, this function only causes errors for the application, not the entire computer like SetWindowsText.

Gerzi confirmed the following Windows terminals are affected by the DoS issue:

1. PuTTY - vulnerability CVE-2021-33500 (freezes the whole computer), fixed in version 0.75.
2. MobaXterm - vulnerability CVE-2021-28847 (app freeze only) is fixed in version 21.0 preview 3.
3. MinTTY (and Cygwin) - vulnerability CVE-2021-28848 (whole computer freeze), fixed in version 3.4.6.
4. Git - uses MinTTY, fixed in version 2.30.1
5. ZOC - vulnerability CVE-2021-32198 (only freezes the application), no fix yet.
6. XSHELL - vulnerability CVE-2021-42095 (freezes the whole computer), fixed in version 7.0.0.76.

Test on web browser

Realizing that most application GUIs use the SetWindowsText function, Gerzi tried to attack popular web browsers like Chrome.

He created an HTML file that could rapidly change the title over and over again, forcing the Chrome browser to freeze. Other browsers using Chrominum kernel such as Edge, Torch, Maxthon, Opera and Vivaldi all froze. Although Firefox and Internet Explorer did not experience the error, performance was also affected.

However, in all cases, the operating system is essentially unaffected by browsers that have a sandbox mechanism. When testing a browser attack inside a virtual machine, this method causes the system to exhaust its resources, leading to a blue screen error.

Feedback from carriers

Google considers the problem that Gerzi reported to be an abuse or stability-related issue, not a security flaw. Meanwhile, Vivaldi blamed the design of Windows 10, which does not limit application memory usage and only uses pagefile (virtual memory) when it runs out of RAM.

Microsoft says it can fix the problem, but it's not far enough to be included in the security update schedule immediately. Microsoft further shared that this problem can only be triggered locally, so the attacker will have to come into contact with the computer. Moreover, due to the nature of the error, which drains resources, the hacker will not be able to trigger anything next and will not be able to exploit beneficial information.

Responding to the above statements, Gerzi said that hackers can remotely trigger the attack by creating a malicious file on the server and then opening it from an unpatched terminal. Hackers may not gain any benefits, but if they hang up at large agencies and corporations at the right time, the damage is also very significant.