

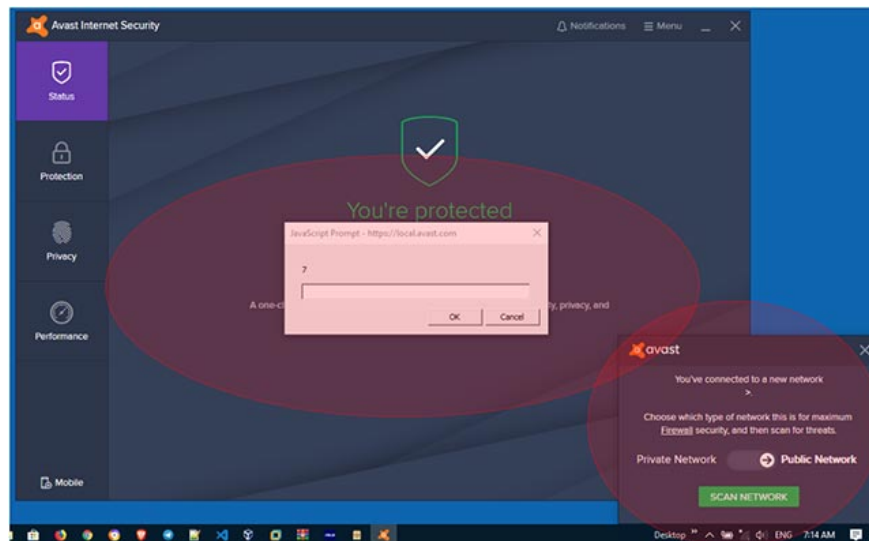
# Serve a serious flaw in Avast Desktop Antivirus Windows application

Detect serious XSS vulnerabilities that appear in Avast Desktop Antivirus application.

In a Medium blog post, a security researcher published a detailed report on the serious XSS vulnerability that appeared in the Avast Desktop Antivirus application he discovered earlier this year. As explained by this expert, an attacker could easily trigger the vulnerability with WiFi SSID.

XSS is one of the common vulnerabilities on applications, especially web applications. Basically, to exploit an XSS vulnerability, an attacker will inject malicious code through scripts to execute on the client. These attacks are often used to bypass access controls and impersonate users.

Back to the vulnerability found on the Avast Desktop Antivirus application for Windows. It is possible for an attacker to attach a malicious payload to an SSID. Then, if a Windows device running Avast antivirus program connects to this WiFi network, an XSS attack will be executed.



The exploitation of this XSS vulnerability is essentially implemented thanks to an integrated feature in the Avast Desktop Antivirus application for Windows itself. By default, the app will display a notification whenever the device tries to connect to a WiFi network without going through any revision laws. So hackers can attach a malicious payload to the SSID name, then execute the malicious code.

After executing the script, a message will be displayed with the content of a fake login prompt created by the attacker. Because users will not be able to see the fake URL, many will enter their login information without even knowing they have been tricked.

The whole process of exploiting the vulnerability is described in the video below:

After the information about the flaw was posted, Avast experts immediately conducted an appraisal and confirmed it was a serious flaw, and offered a \$ 5000 reward to any researcher who gave it. The most optimal patch.

The vulnerability affects not only Avast but also AVG, and is being monitored with the identifier CVE-2019-18653 for Avast and CVE-2019-18654 for AVG.

You finished reading the article "**Serve a serious flaw in Avast Desktop Antivirus Windows application**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.