Subject:- **Prevention Against CCleaner Zero Day flaw (Advisory No 13) October, 2017)**

1. Introduction. CCleaner is a popular utility tool by **Piriform** which is widely used in **Govt/Private organizations.** It is used to **improve system performance** and to **delete redundant files on the system.** Recently the Piriform has informed its users that **hackers have illegally modified the CCleaner v5.33 released in August 15** to compromise the users.

2. **Capabilities of Malware**

a. CCleaner is installed as a trusted application with a valid digital signature so the computer's antimalware solutions doesn't checks it for malicious behaviour.

b. The malware can get the version of CCleaner, name of the computer, list of installed software, including Windows updates, list of running processes and MAC addresses of first three network adapters.

c. The malicious payload of CCleaner can download additional files like keyloggers and ransomeware to further harm the system.

3. **Recommendations**

a. Install and update well reputed and licensed antiviruses like Kaspersky, Avast, BitDefender etc.

b. If you are running **CCleaner v5.33** then disconnect the system from intemet, backup sensitive files and reinstall the operating system.

c. Keep all softwares updated including OS, Microsoft Office, browsers etc.

d. Don't download attachments from emails unless you are sure about the source.

e. Don't click on the pop-ups from random sites.

f. Keep your sensitive files and confidential data on a completely offline system.