CYBER SECURITY ADVISORY – WINRAR VULNERABILITY (ADVISORY NO.69)

1. **Context .** WinRAR application is used for archiving files on windows; supports packing and unpacking of common archive formats (RAR and ZIP). Recently, **a remote code execution** bug has been discovered in WinRAR versions 5.71 and below.

2. **Vulnerability Details**

   a. **CVE Identifier.** CVE -2021 -35052

   b. **Impact**. Bug impacts trial version of WinRAR (version 5.71 and below).

   c. **Consequences.** This vulnerability allows an attacker to intercept and modify requests sent to the user of WinRAR.

   d. **Execution Methodology.** During the exploitation process, masqueraded JavaScript execution script runs and connects with the C&C server.

3. **Recommendations.**

   a. Update WinRAR to version 6.02.

   b. Block script based executions on all endpoints / Internet systems.

   c. Management of third-party software must be controlled through policies and managing the risk associated with external applications.