Subject: **Advisory – Prevention against Critical WINRAR Vulnerability (Advisor No.11)**

1. **Introduction.** Cyber-criminal groups and individual hackers are exploiting old versions of WinRAR software before 5.70 beta 1. Malicious actors can hide the payload into legitimate WinRAR file that can exploit the security of whole system. Therefore, it is advised to upgrade to latest version of WinRAR software or shift to alternative archive utility for Windows.

2. **Summary of Exploit**

   a. **Exploited Software**. WinRAR.

   b. **Affected Versions**. All versions of WinRAR before 5.70.

   c. **Affected Platform**. All version of Windows OS.

   d. **CVE index**. 2018-20250.

3. **Indicators of Compromise**. If the given indicator is found in your system that means the platform is infected **C:\Users\<admin>\AppData\Roaming\Microsoft\Windows\StartMenu\Progr-ams\Startup\<rand>.exe** location.

4. **Technical Details**

   a. Major flaw resides in the code of WinRAR software that handles the extraction of **ACE format files.**

   b. As WinRAR doesn't detect the extension of a file, so attackers just change the **.ace** extension to **.rar** extension to make the compressed file look normal and to gain trust of user.

   c. When victim **right clicks** on the compressed WinRAR file and clicks on **extract here option** then user requested file is extracted along with a malicious payload, that is dropped in the location mentioned in **para 3**.

   d. WinRAR team has now released a WinRAR version 5.70 beta 1 that doesn't support the ACE format, hence protecting users from this attack.

5. **Recommendations**. In order to safeguard the users from WinRAR based malicious attacks, following are recommended:-

   a. Immediately uninstall old versions of WinRAR and install latest version of WinRAR 5.70 (or above) or **utilization of alternative software like WinZip, or 7Zip** is also recommended.

   b. **Install and update well reputed licensed antivirus / antimalware** solution like Kaspersky, AVAST, AVIRA etc.

c. Avoid opening files received from unknown sources and **immediately report malicious / suspicious emails on addresses** mentioned in **para 6**.

d. Uninstall and **remove all unwanted applications** from your Windows platform and Android phone.

e. **It is mandatory for all users to utilize 2x factor authentication on all emails, social media and banking accounts.**

f. **Network, Domain and Host based firewalls must be activated on all endpoints.**