RAJASTHAN RAJYA VIDYUT PRASARAN NIGAM LIMITED
(AN ISO 9001:2015 CERTIFIED COMPANY)
Corporate Identity Number (CIN):U40109RJ2000SGC016485
OFFICE OF THE SUPERINTENDING ENGINEER (MIS&IT)
IT CENTRE, Chambal Power House Premises, Hawa Sarak Sodala, Jaipur
Email: se.mis@rvpn.co.in, Phone No: 0141-2393814

No./RVPN/SE/ (MIS&IT)/XEN-I/AEN/F.71 (2021) (5)/D.301 Date: 7/7/21

All System Users,
RVPN.

Subject: Regarding adopting best cyber security practices in RVPN.

In reference to the advisories issued by the CERT-IN and NCIIPC some important security measures are to be adopted in RVPN to make the network environment safe and secure. Various product advisories are received and in regard of that kindly adopt the practices as listed below:

1. Multiple vulnerabilities have been reported in Adobe Acrobat and Reader which could allow an attacker to execute arbitrary code on the target system.

   Apply appropriate patches as mentioned in below link:

   https://helpx.adobe.com/security/products/acrobat/apsb21-37.html

2. Users are advised to not click on the direct links in email which are redirecting you to some external page. Always observe the URL and in case of some doubt the issue may be escalated to this office with all details of the incident so that such IP and sends are blocked at the Firewall end. Kindly follow the guidelines below in this regard:

   a. As a thumb rule, never click on links received in emails, even from a known / official source, instead, type or copy/paste the link in a browser tab for access.
   b. Keep the mouse pointer over the link for a second or two (mouse over) and the actual link will be displayed on screen, which can be compared to the link appearing in the mail to ascertain authenticity.
   c. Ensure that the computer / device used to access the mail have an updated OS, updated Antivirus software. Carry out a full scan of the host machine every week to check for the presence of malware.
   d. 'Remember password' option not be checked/ enabled/ configured on mail access applications (browser / MS-Outlook / etc.) on any device including official PC.
   e. User/ Custodian of email to change passwords at regular intervals (15 days is recommended). Passwords to have 8-15 character length contain at least one Capital character, one special char and one numeric char in a difficult to guess combination. Ensure change of password from a clean system; refrain from changing on a public device / mobile phone.

f. Discard/ Delete spam/ unknown or suspected phishing emails mails after forwarding a copy to se.mis@rvpn.co.in for analysis.

3. Multiple vulnerabilities have been reported in Google Chrome which could allow a remote attacker to execute arbitrary code or bypass security restrictions on the targeted system. Successful exploitation of these vulnerabilities could allow the attacker to execute arbitrary code or bypass security restrictions on the targeted system resulting in complete system compromise. Kindly Upgrade to Google Chrome 91.0.4472.114 mentioned in the link below.

   https://chromereleases.googleblog.com/2021/06/stable-channel-update-for-desktop_17.html

4. Multiple vulnerabilities have been reported in various Microsoft products, which could be exploited by an attacker to access sensitive information, bypass security restrictions, perform a denial of service (DoS) attack, escalating privileges, perform Spoofing attacks or execute arbitrary codes on the targeted system. An upgrade to Microsoft Office is also recommended from link https://msrc.microsoft.com/update-guide/releaseNote/2020-Jun.

5. Vulnerability in Print Spooler service of Microsoft Windows, being termed as "Print Nightmare", has been reported which could be exploited by a remote attacker to execute arbitrary code on a targeted system.

   Microsoft is currently assessing the vulnerability and no patches are available yet. Users are advised to check the following webpage for updates:

   https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

Manish Athaiya 7/7/2021

(Manish Athaiya)
Superintending Engineer (MIS & IT),
RVPN, Jaipur

Copy to Addl. Chief Engineer (IT), RVPN, Jaipur for kind information:

Manish Athaiya 7/7/2021

Superintending Engineer (MIS & IT),
RVPN, Jaipur