

**Subject: Cyber Security Advisory – Ransomware Attacks on VMWare ESXi Unpatched Servers (Advisory No. 04)**

**Context.** VMWare ESXi hypervisors are the target of a new wave of attacks designed to deploy ransomware on compromised systems. These attack campaigns appear to exploit CVE-2021-21974 (heap overflow vulnerability allowing remote code execution). A patch is available. Users and Administrators are requested to examine and apply necessary updates as per recommendation mentioned at Para-2.

2. **Recommendation**

- a. For detailed information regarding vulnerability of IT/Network, Admins are advised to visit [www.vmware.com/security/advisories.html](http://www.vmware.com/security/advisories.html) and [www.vmware.com/support/services/production.html](http://www.vmware.com/support/services/production.html).
- b. Administrators and Users are requested to apply security patches by updating VMWare ESXi to latest available version (7.0).