البنك المركزي الأردني
Central Bank of Jordan

JO-FinCERT – Security Advisory – 2023 – 44

1. Chinese hackers used VMware ESXi zero-day to backdoor VMs

Chinese hackers utilized a zero-day vulnerability in VMware ESXi servers, enabling them to gain unauthorized access and implant malware into virtual machines (VMs). The specific initial access technique and the motivation behind the attack remain unclear. The infection's impact could involve unauthorized access to sensitive data, data manipulation, service disruption, or further exploitation of the compromised systems. The affected systems primarily include the VMware ESXi servers and the VMs hosted on those servers.

1. CVE-2023-20867: A fully compromised ESXi host can force VMware Tools to fail to authenticate host-to-guest operations, impacting the confidentiality and integrity of the guest virtual machine. CVSS of 3.9/Low

Reference: https://www.mandiant.com/resources/blog/vmware-esxi-zero-day-bypass

2. Microsoft June 2023 Patch Tuesday fixes 78 flaws including 38 RCE bugs

Microsoft's June 2023 Patch Tuesday release aimed to address 78 vulnerabilities, including 38 Remote Code Execution (RCE) bugs, impacting a range of Microsoft products and services. While there are no zero-day vulnerabilities, there are some notable flaws listed below:

1. CVE-2023-29357: Microsoft SharePoint Server Elevation of Privilege Vulnerability. CVSS of 9.8/Critical
2. CVE-2023-32031: Microsoft Exchange Server Remote Code Execution Vulnerability. CVSS of 6.5/Medium

Recommendations: It is crucial to apply these patches promptly to avoid issues.

Reference:https://www.bleepingcomputer.com/news/microsoft/microsoft-june-2023-patch-tuesday-fixes-78-flaws-38-rce-bugs/