Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No. 243 **14-3-2024**

Name: Microsoft SCCM Misconfigurations Usable in Cyberattacks

Threat Classification: Misconfiguration Vulnerability

Affected Software / Area:

- Microsoft's Configuration Manager (formerly known as System Center Configuration Manager - SCCM)

Summary:

Security researchers have unveiled a repository called Misconfiguration Manager, focusing on attack and defense techniques stemming from improperly configured Microsoft Configuration Manager (MCM). MCM, a stalwart presence in Active Directory environments since 1994, aids administrators in managing servers and workstations on Windows networks. However, its default configurations have long been scrutinized as potential attack surfaces for adversaries seeking administrative privileges within a Windows domain.

The researchers emphasize that MCM/SCCM setup is complex, often leading to default configurations that offer exploitable openings for attackers. Notably, the repository (https://github.com/subat0mik/Misconfiguration-Manager) outlines scenarios where misconfigured MCM deployments facilitated attackers' routes to domain controller status, exploiting overprivileged Network Access Accounts (NAAs) and mismanagement of Configuration Manager sites.

Attack and defense methodologies detailed in the Misconfiguration Manager repository aim to provide insights for administrators into MCM's intricacies and streamline attack path management. Presently, the repository catalogs 22 techniques for direct attacks on MCM/SCCM or its exploitation in post-exploitation phases. Defense strategies are categorized into prevention, detection, and canary tactics to mitigate the identified vulnerabilities.

Severity	**High**
Attack Vector	Remote Code Execution

Recommendations:

- Implement guidance and strategies for detecting various attack techniques.
- Deploy detection strategies based on deception, leveraging features attackers commonly abuse.
- In case of any incident, please report to this office, through PTA CERT Portal and email.