Report Title: Cyber Incident Report

Incident Date and Time: 23/03/23, 21:22

Incident Location: DCServ2

Description of Incident:

On 23/03/23, 21:22 the SOC detected a suspicious activity on DCServ2, indicating a potential cyber attack. After further investigation, it was determined that the attacker gained unauthorized access to the system by exploiting a vulnerability in DCServ2, using CVE-2022-31547. The attacker then proceeded to exfiltration hashed passwords from the system.

Impact Assessment:

The cyber attack resulted 127 hashed passwords being compromised. The financial impact of the incident is estimated to be minimal, and the potential reputational damage to the organization is medium.

Response Actions:

Upon detection of the incident, the SOC immediately initiated the incident response process, including containment, investigation, and remediation efforts. The compromised system was taken offline, and affected users were notified. The SOC worked with IT and other departments to conduct a thorough review of all systems and implement additional security measures to prevent further incidents.

Root Cause Analysis:

The root cause of the incident was determined to be a vulnerability in DCServ2, which was not patched in a timely manner. The attacker was able to exploit this vulnerability and gain unauthorized access to the system, including remote code execution. The organization has since implemented a patch management process to ensure timely updates are applied to all systems.

Recommendations:

To prevent similar incidents in the future, the SOC recommends the following measures:

Implement a comprehensive vulnerability management program to regularly scan for and patch vulnerabilities.

Implement a data loss prevention solution to help detect and prevent exfiltration of sensitive data.

Change passwords for all users.

Conclusion:

The SOC has successfully responded to the cyber incident and implemented measures to prevent similar incidents in the future. It is important that the organization remains vigilant and continues to prioritize cyber security, such as implementing patching and updates, to protect its assets and data.