Cyber Security Report on Online Registration and Attendance System (ORAS)

Overview of the System

The Online Registration and Attendance System (ORAS) is a web-based application developed by the DOST-MIMAROPA MIS Unit. ORAS automates the registration of participants for training and meetings and facilitates the attendance tracking of Work-From-Home (WFH) employees. The system is essential for streamlining operational processes related to participant registration and employee attendance management.

Incident Summary

On October 29, 2024, a cyberattack targeted ORAS, specifically exploiting user login credentials and uploading malicious files. The attacker used multiple IP addresses and successfully compromised the system by brute-forcing a user account. This report summarizes the events, identified vulnerabilities, and corrective actions taken.

Key Details of the Attack

- Date and Time of Initial Attack: October 29, 2024, at 11:50 PM

- Method: Brute-force login attack on Carl Francis Javate's account

- Key Actions by Attacker:
    - Successfully uploaded a profile image and malicious file at 12:14:51 to exploit the file upload feature.
    - Attempted unauthorized folder access at various times, notably at 12:26:05 and later at 22:12:47.
    - Logged in to compromised accounts from 22:03:40 to 22:08:32 on October 29, 2024.
    - Re-login attempt noted on November 4, 2024, at 00:35:47.

- Malware Detection and Removal: Hostinger's Malware Scanner automatically detected and removed the malicious file at 4:39 AM on October 29, 2024.

- IP Addresses Used:
    - United States: 38.46.223.55
    - Japan: 45.87.213.230
    - Republic of Korea: 20.196.197.70

Mitigation and Corrective Actions

Upon discovering the incident, the following steps were taken on November 4, 2024, at 09:45 AM:

1. Inspected the file manager on the hosting server and removed unauthorized HTML files that have been uploaded.
2. Updated login credentials for all accounts to prevent further unauthorized access.
3. Temporarily took down the system for maintenance and security reviews.
4. Uploaded an updated `index.php` file, enabling the admin to check for any signs of defacement or further modifications on the website.
5. Verified that the PHP version is updated to version 8.1, minimizing risks associated with outdated software.
6. Strengthened file permissions, updating critical files from 755 to 555 to prevent unauthorized modifications.

Due to the ORAS system's inactivity since 2022—when it was last used for tracking Work-From-Home attendance during the pandemic—it is recommended to formally decommission or replace the system. As an immediate corrective action following the recent security incident, the system was temporarily taken offline.