Security Incident Report

Risk Assessment Results

Identified Assets

- The organization owns one Server and several workstations, routers, switches, and other hardware devices.
    - Applications include various software systems such as HRIS (Human Resources Information System), CRM (Customer Relationship Management), and ERP (Enterprise Resource Planning) systems.

Incident Report: WordPress Website Attack

Date: October 8, 2024

Time: 07:35 AM

Victim: 4Geeks Server

- **Server Configuration**
    - **Operating System:**
        - Debian Bookworm (Debian 12)
    - **Services:**
        - Web server (Apache/NGINX)
        - Database server (MySQL/MariaDB)
        - File storage server (Samba/SFTP)
        - Application servers (Node.js, PHP)

Attacker IP: 192.168.0.134

Description: A malicious actor exploited a WordPress vulnerability to gain unauthorized access to the 4Geeks server. The attacker targeted the WordPress installation and exfiltrated sensitive files, including `wp-config.php`, which contained database credentials.

Attack Details:

1. **System Enumeration:**
    - The attacker identified the WordPress version through directory traversal or file content analysis using nmap and wpscan.
2. **Sensitive Information Gathering:**
    - The attacker extracted `wp-config.php`, which contains database credentials, indicating an attempt to gain access to the backend and manipulate data.
3. **Data Exfiltration:**

    - Sensitive files were exfiltrated from `/var/www/html` directory, including WordPress core files, plugins, themes, and media assets.

Impact:

- Sensitive data exposure: The attacker gained access to database credentials, which could have led to unauthorized access and manipulation of sensitive data.
- Data loss: The attacker exfiltrated media assets, which could have been used for further attacks or to compromise reputation.

Mitigation:

- Patch the WordPress installation to the latest version.
- Implement strong password policies and multi-factor authentication for user accounts.
- Keep all system and application logs for monitoring and alerting.
- Regularly review and update the security policies and procedures.

Recommendations:

- Implement a firewall to protect the server from external attacks.
- Limit access to the WordPress installation to only necessary IP addresses and ports.
- Regularly backup the database and test the restoration process.
- Encrypt sensitive data at rest and in transit.
- Conduct security awareness training for all employees to recognize and report suspicious activities.

Timeline:

- **08/Oct/2024:16:49:46**: Attacker identified and modified WordPress directories.
- **08/Oct/2024:08:01**: Attacker identified and modified WordPress directories.
- **08/Oct/2024:08:01**: Attacker extracted `wp-config.php`.
- **08/Oct/2024:09:27 - 09:56**: Attacker exfiltrated files and directories.

This incident report provides a comprehensive overview of the attack, its impact, and the steps taken to mitigate the risks. It also highlights the importance of maintaining a robust security program and having a comprehensive incident response plan in place.