ABSTRACT

Systematic Analysis of Adobe Coldfusion Vulnerability Incidents With Risk Mitigation and Mitre Attack Methodology

By:

Mulkan Azhiman

6705210049

Research on the Adobe ColdFusion Exploit Incident Leading to System Compromise at a Client Company. A recent incident involving the Adobe ColdFusion exploit resulted in a system compromise at a client company. This incident caused significant financial and reputational damage to the company. This research aims to analyze the root cause of the incident, its impact, and mitigation and prevention measures that can be implemented.

The primary objectives of this research are systematically analyze the incident using the MITRE ATT&CK framework and Formulate risk mitigation strategies to prevent similar incidents.

This research employs a case study methodology, utilizing log analysis and incident-related documentation. The MITRE ATT&CK framework is adopted to identify the tactics, techniques, and procedures (TTPs) employed during the incident.The research findings indicate that the incident was exploited using MITRE ATT&CK tactics and techniques.

The overall analysis suggests that the incident was attributed to a combination of factors, including:

1. Vulnerabilities in the Adobe ColdFusion software used by the company.
2. Inadequate security controls and monitoring of systems utilizing Adobe ColdFusion.
3. Misconfigurations and insufficient patch management practices.

Based on the findings, the research recommends the following mitigation and prevention measures to avert similar incidents:

1. Update Adobe ColdFusion software to the latest secure version.
2. Implement adequate security controls and monitoring for systems using Adobe ColdFusion.
3. Enhance employee cybersecurity awareness and training.
4. Establish and enforce effective patch management policies.

This research aims to provide insights into the Adobe ColdFusion exploit incident leading to system compromise and assist companies in enhancing their cybersecurity posture. By implementing the recommended mitigation and prevention measures, organizations can effectively safeguard their systems and data from similar attacks.

keywords: *adobe coldFusion, exploit, system compromise*, mitigation, prevention, cybersecurity