

CVE-2024-1234: PDF JavaScript Injection Analysis

Abstract

In this paper we describe a vulnerability in which a malicious PDF uses a /JavaScript action to execute arbitrary code. The eval() function is called with attacker-controlled input. Remediation: patch the reader to ignore /JavaScript actions in /OpenAction.