# Searchlight Cyber Finds Three Cross-Site Scripting Vulnerabilities in Adobe Experience Manager

*Vulnerabilities could have been used to exploit all 45k sites running the cloud version of AEM*

BRISBANE, AUSTRALIA, July 1, 2025 /EINPresswire.com/ -- The Assetnote Security Research Team at Searchlight Cyber has published the details of three consecutive persistent Cross-Site Scripting vulnerabilities that it uncovered in the cloud version of the Adobe Experience Manager (AEM) Content Management System (CMS). Each one of these could have been exploited in the 45,000 sites running the cloud version of AEM.

The three vulnerabilities (grouped into two CVEs: CVE-2025-47114 and CVE-2025-47115) were responsibly disclosed to Adobe and have been patched for all customers.

AEM is used by many large enterprises to manage their websites and the Assetnote Security Research Team found the first vulnerability while conducting a bug bounty on a site using the software. The researchers noticed that AEM was running “at edge” services, which are outside the control of AEM cloud users, and hypothesized that these could be exploited to allow Cross-Site Scripting (also known as XSS). XSS is a type of attack that allows hackers to inject malicious scripts into websites, potentially compromising user interactions and data.

As each patch was applied by Adobe, the researchers tested the application again and found another work around. In total, the researchers managed to exercise XSS three times, each with the potential to impact all websites running on AEM. The three vulnerabilities were disclosed and patches made between April 25, 2025 and June 10, 2025. A detailed description of how these vulnerabilities were uncovered can be found on the Assetnote Security Research Center.

Shubham Shah, SVP of Research and Engineering at Searchlight Cyber commented: “Modern cloud-based applications can often contain many components that are not immediately in the control of users, such as services hosted on CDNs or the edge. When these components are

susceptible to vulnerabilities, users of these platforms can inadvertently find themselves vulnerable to exploitation without the ability to quickly or effectively remediate these issues. This series of XSS vulnerabilities that we discovered in the Adobe Experience Management illustrate the challenges created by modern application design and the need for rigorous security testing."

Searchlight Cyber's security research team continues to perform novel zero-day and N-day security research to ensure maximum coverage and care for its customers' attack surfaces. All research is integrated into its Attack Surface Management platform, Assetnote, which continuously monitors, detects, and proves the exploitability of exposures before threat actors can use them.

About Searchlight Cyber:

Searchlight Cyber was founded in 2017 with a mission to stop threat actors from acting with impunity. Its External Cyber Risk Management Platform helps organizations to identify and protect themselves from emerging cybersecurity threats, with Attack Surface Management and Threat Intelligence tools designed to separate the signal from the noise. It is used by some of the world's largest enterprises, government and law enforcement agencies, and the Managed Security Service Providers at the forefront of protecting customers from external threats. Find out more at www.slcyber.io.

Sonia Awan
Outbloom Public Relations
soniaawan@outbloompr.net
Visit us on social media:
LinkedIn

This press release can be viewed online at: https://www.einpresswire.com/article/827347359

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.
© 1995-2025 Newsmatics Inc. All Right Reserved.