SEARCHLIGHT CYBER UNCOVERS HIGH SEVERITY REMOTE CODE EXECUTION VULNERABILITY IN POPULAR SURVEY SOFTWARE

Users of the Lighthouse Studio survey software should update to the latest version urgently

BRISBANE, AUSTRALIA, July 17, 2025 /EINPresswire.com/
--
- The Assetnote Security Research Team at Searchlight Cyber has published the details of a Remote Code Execution (RCE) vulnerability it discovered in the popular survey software Lighthouse Studio, developed by Sawtooth Software. The vulnerability CVE-2025-34300 was reported to the company in April 2025 and has been patched in Version 9.16.14.

Lighthouse Studio is a survey software widely used by enterprises and often hosted on-premise. The security researchers uncovered the template injection vulnerability in the Perl CGI scripts, which are uploaded to a company's website to allow users to take the survey. This vulnerability would allow an unauthenticated attacker to execute arbitrary commands in the underlying web server via the Lighthouse Studio software. A detailed description of how this critical vulnerability was uncovered can be found on the Assetnote Security Research Center.

The potential impact of this vulnerability is particularly significant, as the scripts lack an auto-update mechanism and are often copied from survey to survey. A single company might have tens or even hundreds of copies of the scripts on their web server. Companies using Lighthouse Studio are urged to manually update to the latest software version (9.16.14) as soon as possible.

Shubham Shah, SVP of Research and Engineering at Searchlight Cyber said: “We were surprised to discover the prevalence of this survey software. For a sense of its popularity, readers can search their email for 'ciwweb' - they may be surprised at the number of results. Moreover, the

payload we discovered works for almost every ‘in the wild’ version of the software. Many companies are using Lighthouse Studios on-premise, so we urge them to manually update the software to avoid falling victim to exploitation.”

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 cybercriminal 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