Assetnote Researchers Discover Zero-Day (CVE-2024-56145) in Craft CMS

BRISBANE, AUSTRALIA, December 20, 2024 /EINPresswire.com/ -- A critical security vulnerability has been discovered by Assetnote in Craft CMS that could allow unauthenticated attackers to execute arbitrary code on affected systems.

Assetnote

Craft CMS is one of the world's most popular content management systems used by over 150,000 websites globally. The vulnerability affects Craft CMS installations running versions prior to 5.5.2 and 4.13.2 when using PHP's default configuration settings.

On November 19th, Assetnote's security research team responsibly disclosed to the Craft CMS team that installations with PHP's default configuration could allow attackers to execute arbitrary system commands without authentication. This vulnerability was promptly patched by the Craft CMS team within 24 hours of responsible disclosure and has been assigned CVE-2024-56145.

"We perform 0-day research on the third-party products our Attack Surface Management customers rely on as a way to continuously improve our platform’s findings through novel research," said Shubham Shah, CTO and Co-founder at Assetnote. "We appreciate Craft CMS’ shared commitment to our customers and their swift response to the disclosure, as they fixed the issue within the first 24 hours."

Key Points:

- Affects Craft CMS installations running versions prior to 5.5.2 and 4.13.2
- Requires PHP's register_argc_argv setting to be enabled (default configuration)
- Allows unauthenticated remote code execution
- Can be mitigated by upgrading Craft CMS or disabling register_argc_argv

Affected Versions

- Craft CMS versions prior to 5.5.2
- Craft CMS versions prior to 4.13.2

Impact:

The vulnerability allows unauthenticated remote attackers to achieve Remote Code Execution (RCE) by exploiting PHP's register_argc_argv configuration setting in conjunction with Craft CMS's command-line argument handling. Craft CMS is used by over 150,000 websites worldwide, making this a significant security concern for many organizations.

Technical Details:

The vulnerability stems from Craft CMS's handling of command-line arguments in its bootstrap process. When PHP's register_argc_argv setting is enabled (which is the default configuration), attackers can manipulate the application's file path handling by passing specific query parameters. This can be leveraged to execute arbitrary code through template injection.

Customers of Assetnote were responsibly notified of vulnerable Craft CMS instances in their infrastructure through an early warning system in the Assetnote Attack Surface Management platform. They were able to see verified proof of exploitability so they could mitigate the exposure. The technical analysis and detailed vulnerability report are available on Assetnote's research blog.

About Assetnote:

Assetnote provides industry-leading attack surface management and adversarial exposure validation solutions, helping organizations identify and remediate security vulnerabilities before they can be exploited. Through continuous security testing and verification, Assetnote enables organizations to actionably defend their attack surface without noise. Assetnote customers receive security alerts and mitigations at the same time to disclosure to third-party vendors.

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