Searchlight Cyber Uncovers High Severity Vulnerability in Open-Source Web Content Management Platform, DNN

The vulnerability is present in multiple software versions (6.0.0 - 10.0.1) and has a severity score of 8.6

BRISBANE, AUSTRALIA, July 8, 2025 /EINPresswire.com/ -- The Assetnote Security Research Team at Searchlight Cyber has uncovered a high severity (CVSS 8.6) vulnerability in the open-source web content management platform DNN (formerly known as DotNetNuke), tracked as CVE-2025-52488. A detailed research post demonstrates how a series of malicious interactions can expose NTLM hashes, which in some cases can be relayed to authenticate to systems that accept NTLM-based authentication. DNN has patched the vulnerability following Searchlight's disclosure.

DNN is a long-standing open-source content management system, established in 2003, written in C# (.NET), and maintained by an active community. It is believed to be used in more than 50,000 websites, including many enterprises.

Searchlight disclosed the vulnerability CVE-2025-52488 in April 2025. The vulnerability was uncovered through the exploitation of a series of quirks in Microsoft, .Net. A detailed description of how this critical vulnerability was uncovered can be found on the Assetnote Security Research Center at https://slcyber.io/assetnote-security-research-center/abusing-windows-net-quirks-and-unicode-normalization-to-exploit-dnn-dotnetnuke/

Ultimately, undertaking this series of actions could have exposed NTLM credentials to an unauthorized actor. The vulnerability is present in software versions 6.0.0 onwards, and has been patched in version 10.0.01.

Shubham Shah, SVP of Research and Engineering at Searchlight Cyber said: "This vulnerability was a complex discovery for our team, as a perfect combination of issues had to align for it to be exploitable. Nevertheless, the bug has existed within DNN across a wide version range and, if it had been identified by a cybercriminal, the damage could have been severe. Enterprises using

DNN should update to the latest version immediately.”

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 cyber criminal 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
