



58,052

VULNERABILITIES SINCE LAUNCH

7,833

RESEARCHERS SINCE LAUNCH

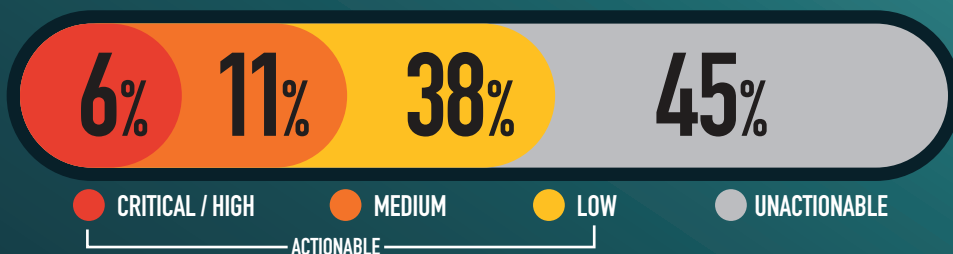
31,468

ACTIONABLE REPORTS PROCESSED

141

ACTIONABLE VDPS FOR THE MONTH

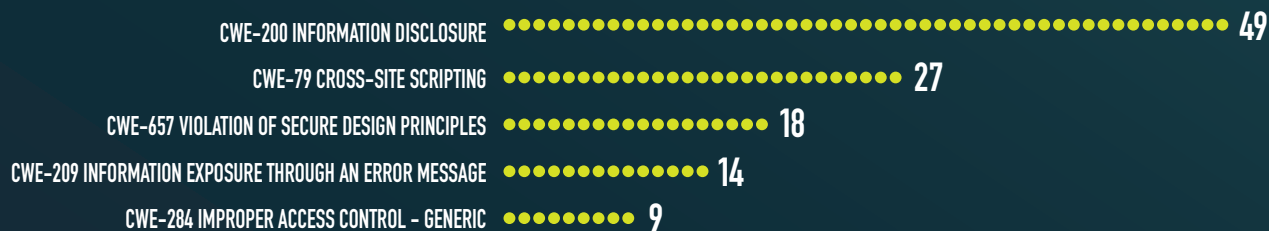
## SEVERITY FOR THE MONTH



## SUBMITTED VULNERABILITIES



## LEADING COMMON WEAKNESS ENUMERATION'S FOR THE MONTH



## KNOWLEDGE BYTE

In November 2025, the DoD VDP received multiple critical severity submissions identifying CVE-2025-64095, an unauthorized file upload capability within DNN. DNN is an open-source content management system and file handler. Researchers identified a publicly available endpoint that could result in the unauthorized overwriting of existing content or uploading of malicious files. It is recommended that all system owners install the latest approved DNN updates. Further information is available in the following resources:

<https://nvd.nist.gov/vuln/detail/CVE-2025-64095>

<https://github.com/dnnsoftware/Dnn.Platform/security/advisories/GHSA-3m8r-w7xg-jqvw>

<https://portswigger.net/web-security/file-upload>

## RESEARCHER OF THE MONTH

Huge congratulations to @0xr2rx for being named Researcher of the Month. @0xr2rx is being recognized for finding a file upload vulnerability, DNN (DotNetNuke), which could have led to arbitrary, unrestricted and unauthorized uploads of any files to the target server. 🏆 Well deserved! #CyberSecurity #VDP