DEFENSE INDUSTRIAL BASE VULNERABILITY DISCLOSURE PROGRAM

MYTE BYTE NOVEMBER 2025

DIB-VDP

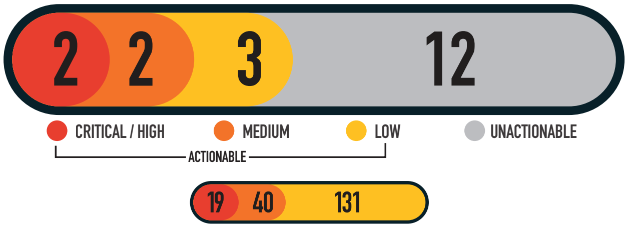
968 VULNERABILITIES SUBMITTED SINCE LAUNCH

13 VULNERABILITIES FOR THE MONTH

257 RESEARCHERS SINCE LAUNCH

7 ACTIONABLE REPORTS PROCESSED

SEVERITY FOR THE MONTH

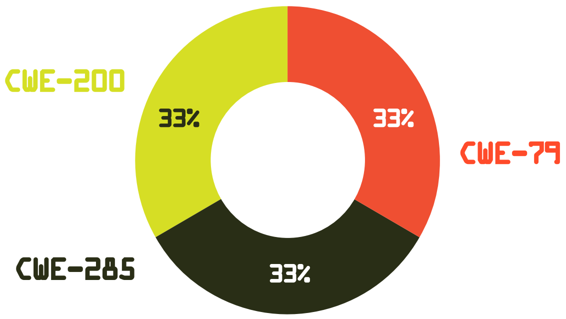


MITIGATED VULNERABILITIES BY SEVERITY SINCE LAUNCH

MITIGATIONS FOR THE MONTH

- ● 7 Successful Mitigations (Including Top 5 Organization Data)
- ● 0 Unsuccessful Attempts

VULNERABILITY TYPES/ LEADING CWE'S FOR THE MONTH



CWE-79 CROSS-SITE SCRIPTING XSS: 1
CWE-285 IMPROPER AUTHORIZATION: 1
CWE-200 INFORMATION DISCLOSURE: 1

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

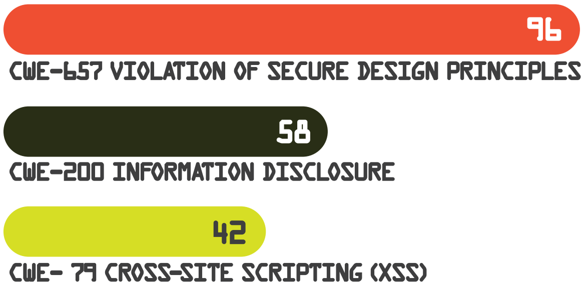
https://github.com/dnnsoftware/Dnn.Platform/security/advisories/GHSA-3m8r-w7xg-jqvw

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

RESEARCHER OF THE MONTH

Big thanks to @wgujjer11 for responsibly disclosing **CVE-2025-64095** in DotNetNuke. This flaw could allow account takeover, data exposure or portal defacement, creating real business and reputation risk if unpatched. **#DIBVDP #CyberSecurity #Infosec #WebSecurity**

TOP VULNERABILITIES SINCE LAUNCH



𝕏 @DC3VDP
AFOSI.DC3.DIB-VDP@us.af.mil

DoD CYBER CRIME CENTER AND DEFENSE COUNTERINTELLIGENCE & SECURITY AGENCY