

MYTE BYTE

DIB-VDP

AUGUST 2021



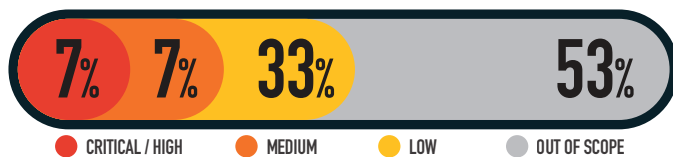
795
VULNERABILITIES
SINCE LAUNCH

146
VULNERABILITIES
FOR THE MONTH

217
RESEARCHERS
SINCE LAUNCH

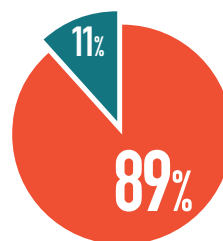
69
ACTIONABLE
REPORTS
PROCESSED

SEVERITY FOR THE MONTH



● CRITICAL / HIGH ● MEDIUM ● LOW ● OUT OF SCOPE

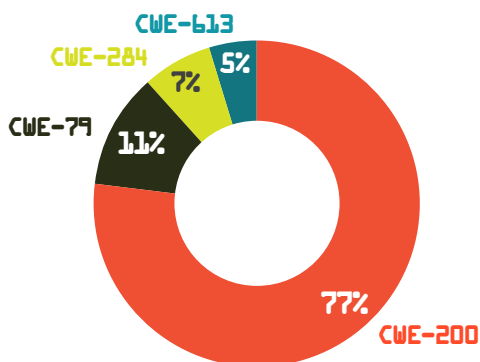
MITIGATIONS FOR THE MONTH



● **31** Successful Mitigations
(Including Top 5 Organization Data)

● **4** Unsuccessful Attempts

VULNERABILITY TYPES/LEADING CWE'S FOR THE MONTH



CWE-200 INFORMATION DISCLOSURE: **67**

CWE-79 CROSS-SITE SCRIPTING (XSS): **10**

CWE-284 IMPROPER ACCESS CONTROL- GENERIC: **6**

CWE-613 INSUFFICIENT SESSION EXPIRATION **4**

KNOWLEDGE BYTE

The DIB-VDP Pilot received a critical severity finding for CWE-312, Cleartext Storage of Sensitive Information. The reported endpoint was found to expose critical financial, tax and billing data as well as a variety of PII and other sensitive technical information. Discovery of this information by a threat actor could possibly lead to fraud, identity threat and social engineering attacks. System owners should test for logic errors in websites that could lead to this CWE, ensure data is encrypted at rest where applicable and apply appropriate access controls. More detail on CWE-312 can be found here:

<https://cwe.mitre.org/data/definitions/312.html>

TOP VULNERABILITIES SINCE LAUNCH

