

MYTE BYTE

DIB-VDP

MAY 2025



784

VULNERABILITIES
SUBMITTED
SINCE LAUNCH

19

VULNERABILITIES
FOR THE MONTH

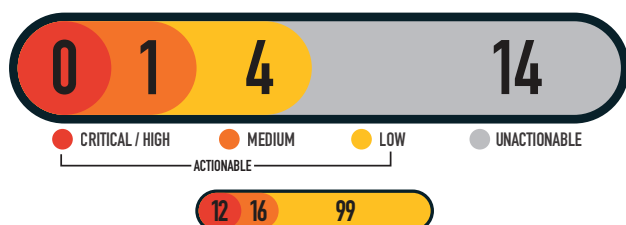
194

RESEARCHERS
SINCE LAUNCH

5

ACTIONABLE
REPORTS
PROCESSED

SEVERITY FOR THE MONTH



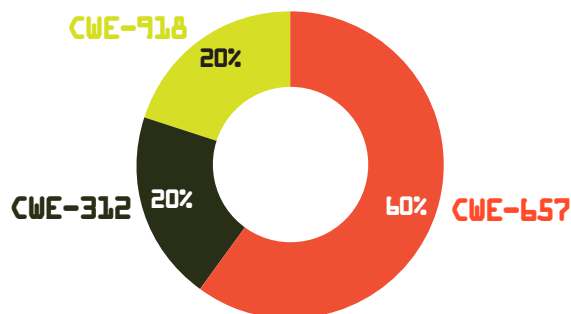
MITIGATED VULNERABILITIES BY SEVERITY SINCE LAUNCH

100%

MITIGATIONS FOR THE MONTH

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

VULNERABILITY TYPES/ LEADING CWE'S FOR THE MONTH



CWE-657 VIOLATION OF SECURE DESIGN PRINCIPLES: 3
CWE-312 CLEARTEXT STORAGE OF SENSITIVE INFORMATION: 1
CWE-918: SERVER-SIDE REQUEST FORGERY: 1

KNOWLEDGE BYTE

In May 2025, the DIB-VDP received a submission outlining the possibility of a Blind Server-Side Request Forgery (SSRF) vulnerability within the login.php page of a common web application. The report suggested that, by manipulating input parameters during the authentication process, an attacker might be able to trigger server-side requests to internal or external resources. The potential impact could include unintended access to internal services or metadata endpoints. System owners are encouraged to validate input and restrict server-side requests to trusted destinations.

Further information is available in the following resources:

https://cheatsheetseries.owasp.org/cheatsheets/Server_Side_Request_Forgery_Prevention_Cheat_Sheet.html
<https://cwe.mitre.org/data/definitions/918.html>
<https://portswigger.net/web-security/ssrf>

RESEARCHER OF THE MONTH

Big thanks to Geison for shedding light on SSRF via Host Header Manipulation! 📺 This attack can bypass security controls, expose sensitive data, and lead to serious breaches. Stay vigilant and secure your headers! 📺
 #DIBVDP #CyberSecurity #InfoSec #WebSecurity #EthicalHacking

TOP VULNERABILITIES SINCE LAUNCH

89

CWE-657 VIOLATION OF SECURE DESIGN PRINCIPLES

41

CWE-200 INFORMATION DISCLOSURE

31

CWE-601 OPEN REDIRECT

