

MYTE BYTE JULY 2024

DIB-VDP



221

VULNERABILITIES SUBMITTED SINCE LAUNCH

77

VULNERABILITIES FOR THE MONTH

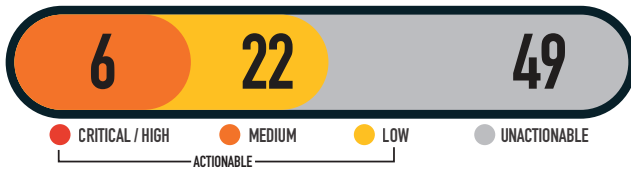
60

RESEARCHERS SINCE LAUNCH

28

ACTIONABLE REPORTS PROCESSED

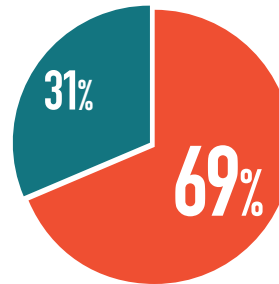
SEVERITY FOR THE MONTH



● CRITICAL / HIGH ● MEDIUM ● LOW ● UNACTIONABLE



MITIGATED VULNERABILITIES BY SEVERITY



MITIGATIONS FOR THE MONTH

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

KNOWLEDGE BYTE

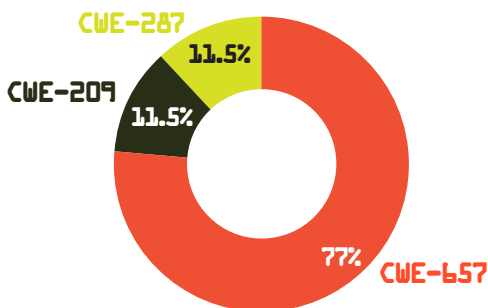
In July 2024, DIB-VDP processed a report concerning a vulnerability in the jQuery library (CVE-2019-11358), which impacts all versions prior to 3.4.0. jQuery is an open-source JavaScript library that simplifies JavaScript coding and is commonly used in many Content Management Systems (CMS). The vulnerability involves a prototype pollution exploit in end-of-life versions of jQuery, which could allow for basic changes to be made to data objects and values, potentially corrupting data or causing application crashes. It is recommended to update jQuery to version 3.4.0 and greater or to ensure the CMS or other framework in use is running at its latest version. More information is available at:

- <https://nvd.nist.gov/vuln/detail/cve-2019-11358>
- <https://attackerkb.com/topics/n4xa4AMDRp/cve-2019-11358>

RESEARCHER OF THE MONTH

🔍 New Discovery! 🔍 **Lucas Pacavira** has found a vulnerability exploiting a Web Application Firewalls (WAF) bypass, allowing unauthorized execution of malicious JavaScript. Mitigate by sanitizing user inputs and updating WAF configurations. 🛡️ #CyberSecurity #InfoSec #OracleWebLogic

VULNERABILITY TYPES/LEADING CWE'S FOR THE MONTH



CWE-657 VIOLATION OF SECURE DESIGN PRINCIPLES: 13
 CWE-209 INFORMATION EXPOSURE THROUGH AN ERROR MESSAGE: 2
 CWE-287 IMPROPER AUTHENTICATION: 2

TOP VULNERABILITIES SINCE LAUNCH

