

# MYTE BYTE

DIB-VDP

JULY 2021



649

VULNERABILITIES  
SINCE LAUNCH

28

VULNERABILITIES  
FOR THE MONTH

194

RESEARCHERS  
SINCE LAUNCH

4

ACTIONABLE  
REPORTS  
PROCESSED

## SEVERITY FOR THE MONTH

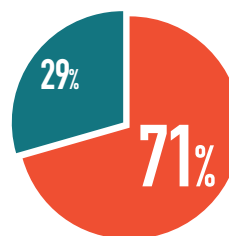


● CRITICAL / HIGH

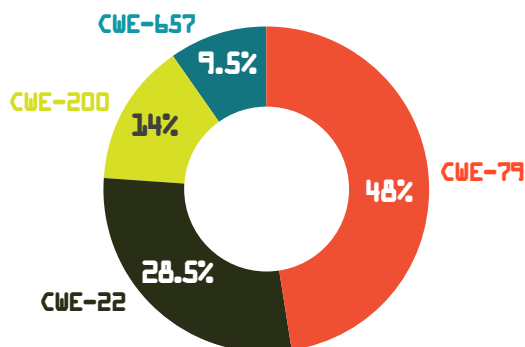
● MEDIUM

● LOW

● OUT OF SCOPE

MITIGATIONS  
FOR THE MONTH● 12 Successful Mitigations  
(Including Top 5 Organization Data)

● 5 Unsuccessful Attempts

VULNERABILITY TYPES/LEADING  
CWE'S FOR THE MONTH

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

CWE-22 PATH TRAVERSAL: 6

CWE-200 INFORMATION DISCLOSURE: 3

CWE-657 VIOLATION OF SECURE DESIGN PRINCIPLES: 2

## KNOWLEDGE BYTE

The DIB-VDP Pilot received notification of CVE-2017-9506, a medium severity exploitable vulnerability in a public-facing asset. The IconUriServlet of the Jira Atlassian OAuth Plugin from version 1.3.0 before version 1.9.12 and from version 2.0.0 before version 2.0.4 allows remote attackers to access the content of internal network resources and/or perform an XSS attack via Server Side Request Forgery (SSRF). When running in an environment like Amazon EC2, this flaw can be used to access a metadata resource that provides access credentials and other potentially confidential information.

<https://nvd.nist.gov/vuln/detail/CVE-2017-9506>

## TOP VULNERABILITIES SINCE LAUNCH

