

# MYTE BYTE

## DECEMBER 2021

DIB-VDP



# 944

VULNERABILITIES  
SINCE LAUNCH

# 17

VULNERABILITIES  
FOR THE MONTH

# 247

RESEARCHERS  
SINCE LAUNCH

# 4

ACTIONABLE  
REPORTS  
PROCESSED

### SEVERITY FOR THE MONTH

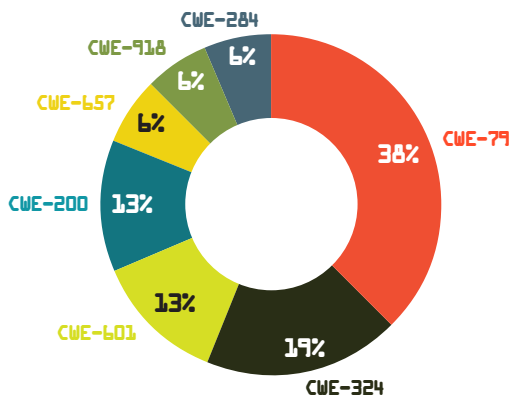


### MITIGATIONS FOR THE MONTH



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

### VULNERABILITY TYPES/LEADING CWE'S FOR THE MONTH



CWE-79 CROSS-SITE SCRIPTING (XSS): 6  
 CWE-324 USE OF KEY PAT ITS EXPIRATION DATE: 3  
 CWE 601 OPEN REDIRECT: 2  
 CWE-200 INFORMATION DISCLOSURE: 2  
 CWE-657 VIOLATION OF SECURE DESIGN PRINCIPLES: 1  
 CWE-918 SERVER-SIDE REQUEST FORGERY (SSRF): 1  
 CWE-284 IMPROPER ACCESS CONTROL- GENERIC: 1

### KNOWLEDGE BYTE

The month of December was taken by storm when the IT world was rocked by the new critical and complex vulnerability that plagued the Apache Log4j library (CVE-2021-44832), aka log4shell. This widely used open-source library effected not only the applications that implemented the library but the services that used those applications. Like most remote code execution (RCE) vulnerabilities the damage can be extensive allowing the attacker to gain full access to the system, steal data, destroy files and infrastructure, and carry out DDoS attacks. System owners are encouraged to either upgrade their systems to Log4j 2.3.2 (for Java 6), 2.12.4 (for Java 7), or 2.17.1 (for Java 8 and later). In particular, system owners should also ensure all 3rd party vendor applications in use have a patch or mitigation available.

For further details on CVE-2021-44832 please visit: <https://logging.apache.org/log4j/2.x/security.html> CISA guidance on Log4J to include impacted vendor list: <https://www.cisa.gov/uscrt/apache-log4j-vulnerability-guidance>

### TOP VULNERABILITIES SINCE LAUNCH

