

# MYTE BYTE

## DIB-VDP

FEBRUARY 2022



1004

VULNERABILITIES  
SINCE LAUNCH

15

VULNERABILITIES  
FOR THE MONTH

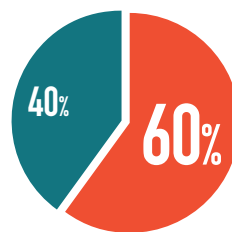
288

RESEARCHERS  
SINCE LAUNCH

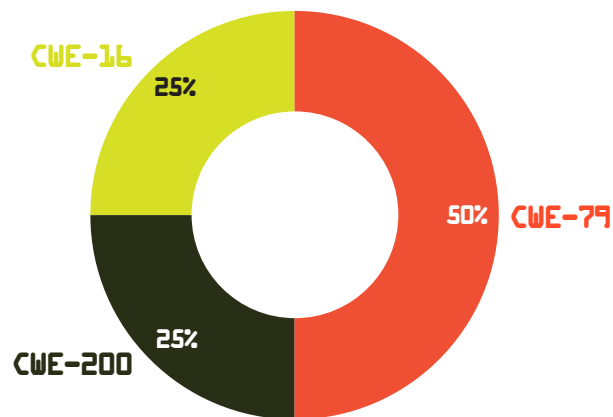
3

ACTIONABLE  
REPORTS  
PROCESSED

## SEVERITY FOR THE MONTH

MITIGATIONS  
FOR THE MONTH

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

VULNERABILITY TYPES/LEADING  
CWE'S FOR THE MONTH

CWE-79 CROSS-SITE SCRIPTING (XSS): 4  
 CWE-200 INFORMATION DISCLOSURE: 2  
 CWE-116 MISCONFIGURATION: 2

## KNOWLEDGE BYTE

DIB-VDP received notification of an asset that shows a server version, Serv-U, in the response header. In this case the finding was taken as a STIG violation but as you will see having the capability to see the server version can quickly escalate into a high or critical finding. This particular server version has known Lightweight Directory Access Protocol (LDAP) sanitization issues tracked through CVE-2021-35247. This vulnerability could allow adversaries to use the Serv-U web login screen to send characters that were not sufficiently sanitized. In a more extreme instance a successful LDAP injection can provide valuable information for further attacks on systems and applications, such as usernames and passwords. For mitigation SolarWinds recommends updating to the latest version of Serv-U. In addition to SolarWinds recommendation we strongly encourage further protection by hiding your server versions so that an escalated attack such as the one mentioned earlier is less likely to occur. For further information the advisory can be found here: <https://www.solarwinds.com/trust-center/security-advisories/cve-2021-35247> & <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35247>

## TOP VULNERABILITIES SINCE LAUNCH

