

# MYTE BYTE

## JANUARY 2022

### DIB-VDP



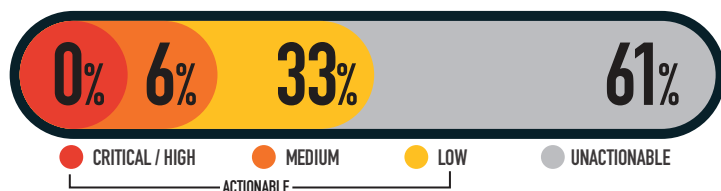
**980**  
VULNERABILITIES  
SINCE LAUNCH

**36**  
VULNERABILITIES  
FOR THE MONTH

**288**  
RESEARCHERS  
SINCE LAUNCH

**14**  
ACTIONABLE  
REPORTS  
PROCESSED

### SEVERITY FOR THE MONTH

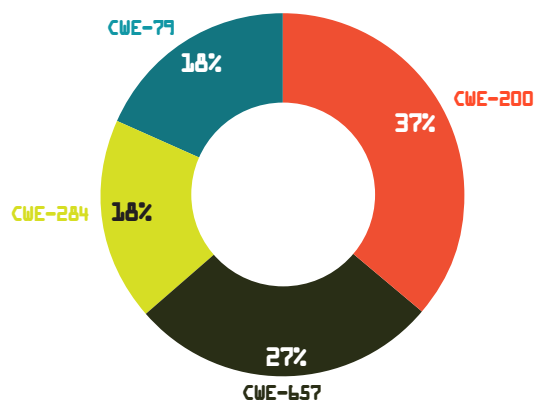


### MITIGATIONS FOR THE MONTH



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

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



CWE-200 INFORMATION DISCLOSURE: 8

CWE-657 VIOLATION OF SECURE DESIGN PRINCIPLES: 6

CWE-284 IMPROPER ACCESS CONTROL- GENERIC: 4

CWE-79 CROSS-SITE SCRIPTING (XSS): 4

### KNOWLEDGE BYTE

DIB-VDP received notification of an asset vulnerable to CVE-2020-3580 which affects the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software and could allow an unauthenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the web services interface of an affected device. The vulnerability is due to insufficient validation of user-supplied input by the web services interface of an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or allow the attacker to access sensitive, browser-based information. Cisco has released software updates that address these vulnerabilities. There are no workarounds that address these vulnerabilities. More information is available at: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3580> & <https://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-asafstd-xss-multiple-FCB3vPZe.html>

### TOP VULNERABILITIES SINCE LAUNCH

