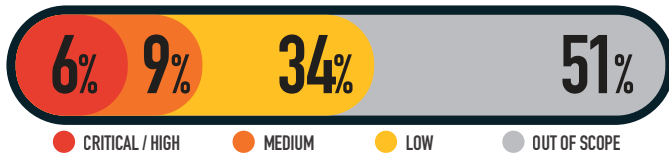**621** VULNERABILITIES SINCE LAUNCH

209 VULNERABILITIES FOR THE MONTH

175 RESEARCHERS SINCE LAUNCH

101 ACTIONABLE REPORTS PROCESSED

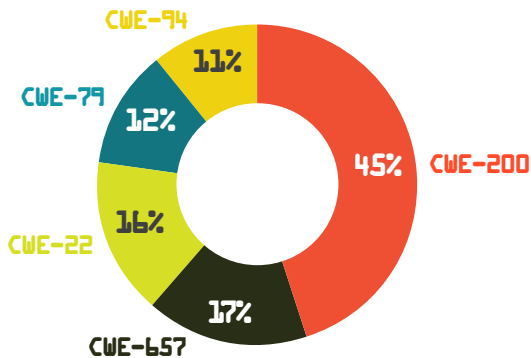## SEVERITY FOR THE MONTH

6% **9%** **34%** **51%**

- CRITICAL / HIGH
- MEDIUM
- LOW
- OUT OF SCOPE

MITIGATIONS FOR THE MONTH

33% 66%
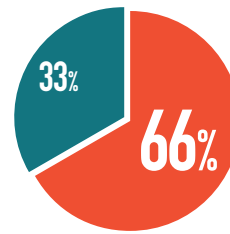
- **24** Successful Mitigations (Including Top 5 Organization Data)
- **12** Unsuccessful Attempts

VULNERABILITY TYPES/LEADING CWE'S FOR THE MONTH

- CWE-94 **11%**
- CWE-79 **12%**
- CWE-22 **16%**
- CWE-657 **17%**
- CWE-200 **45%**

CWE-200 INFORMATION DISCLOSURE: **68**
CWE-657 VIOLATION OF SECURE DESIGN PRINCIPLES: **25**
CWE-22 PATH TRAVERSAL: **24**
CWE-79 CROSS-SITE SCRIPTING (XSS): **18**
CWE-94 CODE INJECTION: **16**

KNOWLEDGE BYTE

DIB-VDP received notification of the following critical severity exploitable finding, CVE-2019-18935, allowing an attacker to upload arbitrary files and gain remote code execution on the underlying system. Progress Telerik UI for ASP.NET AJAX through 2019.3.1023 contains a .NET deserialization vulnerability in the RadAsyncUpload function. This is exploitable when the encryption keys are known due to the presence of CVE-2017-11317, CVE-2017-11357, or other means. Exploitation can result in remote code execution. Please update as soon as possible! Further information is available at:

https://nvd.nist.gov/vuln/detail/CVE-2019-18935
https://iavm.csd.disa.mil/iavm-notice-html/142791

TOP VULNERABILITIES SINCE LAUNCH

CWE-200 INFORMATION DISCLOSURE	**169**
CWE-79 CROSS-SITE SCRIPTING (XSS)	**83**
CWE-657 VIOLATION OF SECURE DESIGN PRINCIPLES	**54**
CWE-22 PATH TRAVERSAL-GENERIC	**40**