



33,413

VULNERABILITIES SINCE LAUNCH

2,798

RESEARCHERS SINCE LAUNCH

20,350

ACTIONABLE REPORTS PROCESSED

## SEVERITY FOR THE MONTH



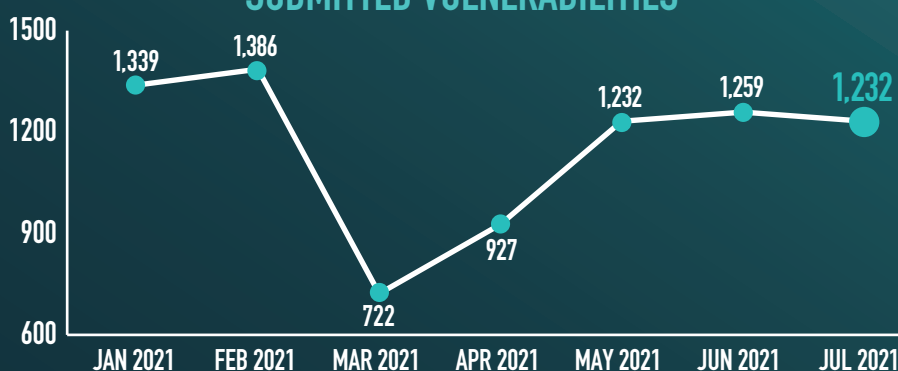
CRITICAL / HIGH

MEDIUM

LOW

OUT OF SCOPE

## SUBMITTED VULNERABILITIES



## LEADING COMMON WEAKNESS ENUMERATION'S FOR THE MONTH

CWE-200 INFORMATION DISCLOSURE 430

CWE-922 INSECURE STORAGE OF SENSITIVE INFORMATION 240

CWE-79 CROSS-SITE SCRIPTING (XSS) 194

CWE-657 VIOLATION OF SECURE DESIGN PRINCIPLE 109

CWE-284 IMPROPER ACCESS CONTROL - GENERIC 41

## KNOWLEDGE BYTE

During the month of July, we received multiple critical submissions regarding vulnerabilities in Telerik UI for ASP.NET AJAX (CVE-2017-11317). Telerik.Web.UI in Progress Telerik UI for ASP.NET AJAX before R1 2017 and R2 before R2 2017 SP2 uses weak RadAsyncUpload encryption, which if successfully exploited, could allow an attacker to execute arbitrary code or file uploads. System owners using an old version of Telerik.Web.UI are encouraged to upgrade to R1 2020 (2020.1.114) or later to prevent the vulnerabilities. There are currently no known DoD related incidents. More information can be found at the following:

<https://iavm.csd.disa.mil/iavm-notice-html/141420> / [https://www.telerik.com/support/kb/aspnet-ajax/upload-\(async\)/details/unrestricted-file-upload](https://www.telerik.com/support/kb/aspnet-ajax/upload-(async)/details/unrestricted-file-upload)

## RESEARCHER OF THE MONTH

We are excited to announce the July 2021 DoD VDP Researcher of the Month Award goes to **Adriano Valle @adrianovalle**. He submitted over 90 reports this month, including high severity Server-Side Request Forgery (SSRF), CVE-2021-22214, that could allow attacks access to a Gitlab server! Keep up the great work and thank you for participating in the DoD Vulnerability Disclosure Program! Happy Hacking!