

BUG BYTES OCTOBER 2022



43,921

VULNERABILITIES SINCE LAUNCH

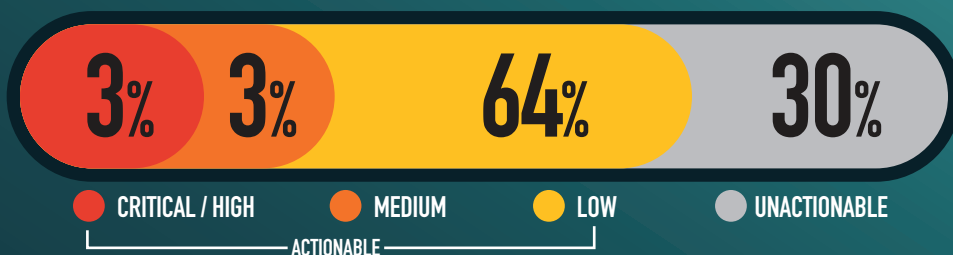
3,795

RESEARCHERS SINCE LAUNCH

25,232

ACTIONABLE REPORTS PROCESSED

SEVERITY FOR THE MONTH



SUBMITTED VULNERABILITIES



LEADING COMMON WEAKNESS ENUMERATION'S FOR THE MONTH



KNOWLEDGE BYTE

In October 2022, the DoD VDP received multiple high and critical severity findings where researchers were able to upload arbitrary files to DoD hosts without restriction. Uploading custom files can lead to many high impact attacks such as Denial of Service via resource exhaustion, credential theft, and command execution. Researchers were able to locate multiple endpoints with the PUT and DELETE methods enabled allowing for the upload and removal of files hosted on the server. As systems grow more complex, it is important for administrators and system owners to regularly audit all public facing endpoints to ensure only necessary HTTP methods are enabled. For further reading on the effects of unsecured file uploads and a full listing of all HTTP methods please see the following:

https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload & <https://portswigger.net/web-security/file-upload> & <https://www.rfc-editor.org/rfc/rfc7231>

RESEARCHER OF THE MONTH

The DoD VDP Researcher of the Month for October 2022 is [@maliciousgroup!](#) They submitted a critical report for unauthorized file uploads on a DoD asset; if not remediated would lead to malicious file execution. Thank you very much! VDP Hackers for the win!