

BUG BYTES JULY 2023



47,222

VULNERABILITIES SINCE LAUNCH

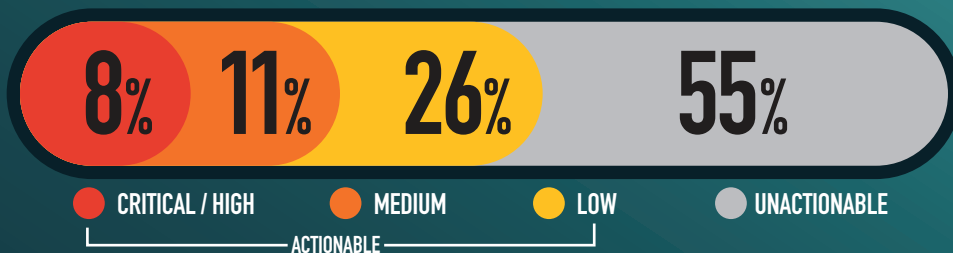
5,015

RESEARCHERS SINCE LAUNCH

27,064

ACTIONABLE REPORTS PROCESSED

SEVERITY FOR THE MONTH



SUBMITTED VULNERABILITIES



LEADING COMMON WEAKNESS ENUMERATION'S FOR THE MONTH

CWE-79 CROSS-SITE SCRIPTING (XSS) 233

CWE-657 VIOLATION OF SECURE DESIGN PRINCIPLES 189

CWE-200 INFORMATION DISCLOSURE 77

CWE-284 IMPROPER ACCESS CONTROL - GENERIC 43

KNOWLEDGE BYTE

In July 2023, The Department of Defense VDP received multiple critical submissions regarding Ivanti Endpoint Manager Mobile (EPMM). A header injection attack allowed for the interception of server responses, potentially exposing sensitive information. System owners deploying Ivanti EPMM are strongly recommended to update to the latest version. For more information, see the following:

<https://www.ivanti.com/blog/epmm-security-concern-with-server-response-leak>

<https://nvd.nist.gov/vuln/detail/CVE-2023-25690>

<https://portswigger.net/research/making-http-header-injection-critical-via-response-queue-poisoning>

RESEARCHER OF THE MONTH

The DoD VDP Researcher of the Month for July 2023 is [@pizzap0w3r](#)! They submitted several critical reports, one being RCE with a Null Byte Truncated File Extension. Impact would have been a full compromise of systems! Thank you very much! VDP Hackers for the win!