

BUG BYTES

OCTOBER 2024



53,393

VULNERABILITIES SINCE LAUNCH

6,839

RESEARCHERS SINCE LAUNCH

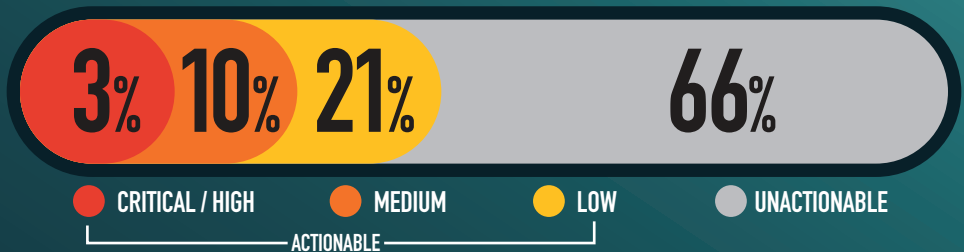
29,391

ACTIONABLE REPORTS PROCESSED

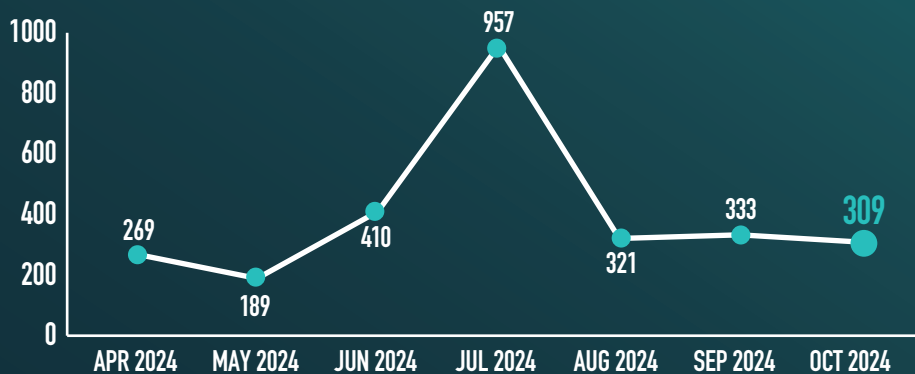
110

ACTIONABLE VDPs FOR THE MONTH

SEVERITY FOR THE MONTH



SUBMITTED VULNERABILITIES



LEADING COMMON WEAKNESS ENUMERATION'S FOR THE MONTH

CWE-284 IMPROPER ACCESS CONTROL - GENERIC 68

CWE-657 VIOLATION OF SECURE DESIGN PRINCIPLES 45

CWE-200 INFORMATION DISCLOSURE 37

CWE-79 CROSS-SITE SCRIPTING 17

KNOWLEDGE BYTE

In October 2024, the DoD VDP received several high severity submissions demonstrating potential access to local system files from servers utilizing Jolokia. Jolokia is a popular Java agent that remotely manages and monitors web applications via API. Researchers identified an endpoint within the Jolokia configuration that could allow for the inclusion and access of sensitive system files. System owners utilizing Jolokia are encouraged to evaluate their endpoint access and regularly update the library. Further information is available in the following resources: <https://jolokia.org/reference/html/manual/security.html>
<https://portswigger.net/web-security/file-path-traversal>

RESEARCHER OF THE MONTH

Security Notice A DoD workstation was unintentionally exposed online. This serves as a critical reminder to always prioritize secure connections. Thanks, [@kalkii_](#), for your vigilance! Let's stay proactive: follow secure protocols and report any anomalies. #CyberSecurity #DoDSecurity