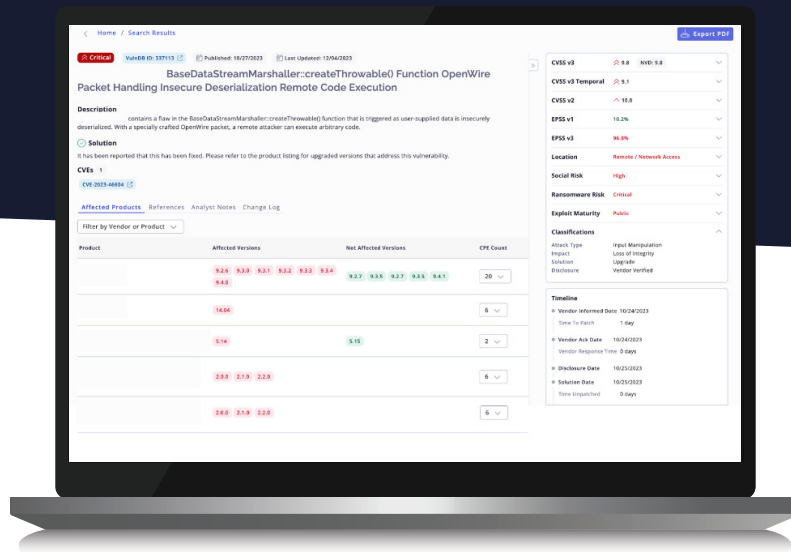# FLASHPOINT

Flashpoint Vulnerability Intelligence

Prioritize & remediate vulnerabilities faster with unparalleled visibility

Flashpoint's Vulnerability Intelligence provides cyber threat intelligence (CTI) teams with unparalleled visibility and context into vulnerabilities– notifying you of vulnerabilities on average two weeks faster than the National Vulnerability Database (NVD) with early coverage of zero-day and emerging vulnerabilities. With timely, comprehensive, evidence-based vulnerability intelligence, CTI teams can confidently assess, prioritize, and reduce vulnerability risk in their environments faster than ever.

Benefits

- ✔ **Identify risk faster** and significantly reduce time to discovery
- ✔ **Leverage accurate and relevant data** to better prioritize vulnerabilities
- ✔ **Collaborate and coordinate across teams** with cyber threat and vulnerability intelligence in one platform
- ✔ **Create internal alignment and confidence** with a single source of truth for vulnerability information

What's included:

REAL-TIME ALERTING ON VULNERABILITIES:

NVD is a powerful resource, but the delay between vulnerability discovery and logging allows bad actors ample time to exploit security gaps. Get ahead of vulnerabilities with earlier coverage and real-time alerting on vulnerabilities. Analysts are alerted about vulnerabilities on average two weeks faster than NVD with early coverage of zero-day and emerging vulnerabilities.

NON-CVES FOR 30% MORE COVERAGE:

Industry-standard vulnerability risk models are likely only 70 percent effective at best. Get comprehensive vulnerability intelligence so your security team can better prioritize threats. Coverage also includes exploit availability, attack vector, and remediation information allowing for the quick targeting of 'easy wins' in patching.

THREAT-BASED RISK SCORES:

Without full context, analysts are limited in their ability to assess threats. Gain a deeper understanding of the scope and potential impact of vulnerabilities with enrichments like EPSS, attribution to exploit intelligence, and social and ransomware risk scores.

UNIQUE ANALYSIS:

Real-world risk involves multiple factors. Leverage expert analysis that covers vulnerabilities with and without CVEs assigned, the full scope of affected products/versions, Linux packages and OSS/3rd party libraries, proprietary severity scoring, extensive classifications and external references, predictive and observed indicators of exploitation, and related threat intelligence.

"Having the Vulnerabilities [feature] in Ignite makes things a lot quicker when researching one that's being actively exploited in the wild." -Pepsico