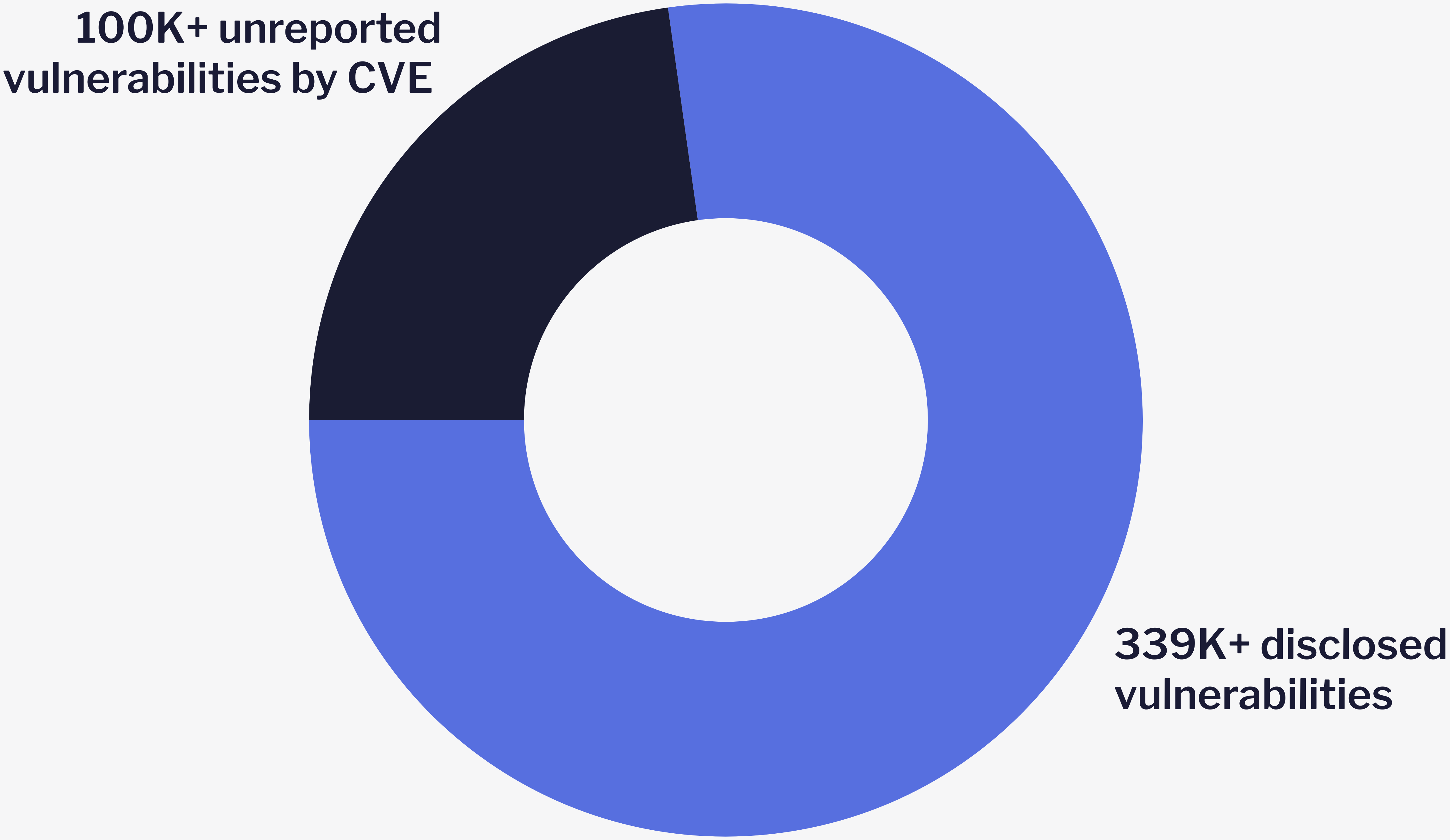
FLASHPOINT

What VulnDB's 100K Non-CVE Vulnerabilities Means For You

Organizations strictly relying on CVE and NVD are likely unaware of nearly a third of all known vulnerability risk.

A critical milestone



VulnDB, Flashpoint’s premier vulnerability intelligence database, hit a critical milestone documenting **over 100,000 vulnerabilities missed by the CVE & NVD databases**.

FLASHPOINT

Here is how this intelligence gap could be affecting your organization:

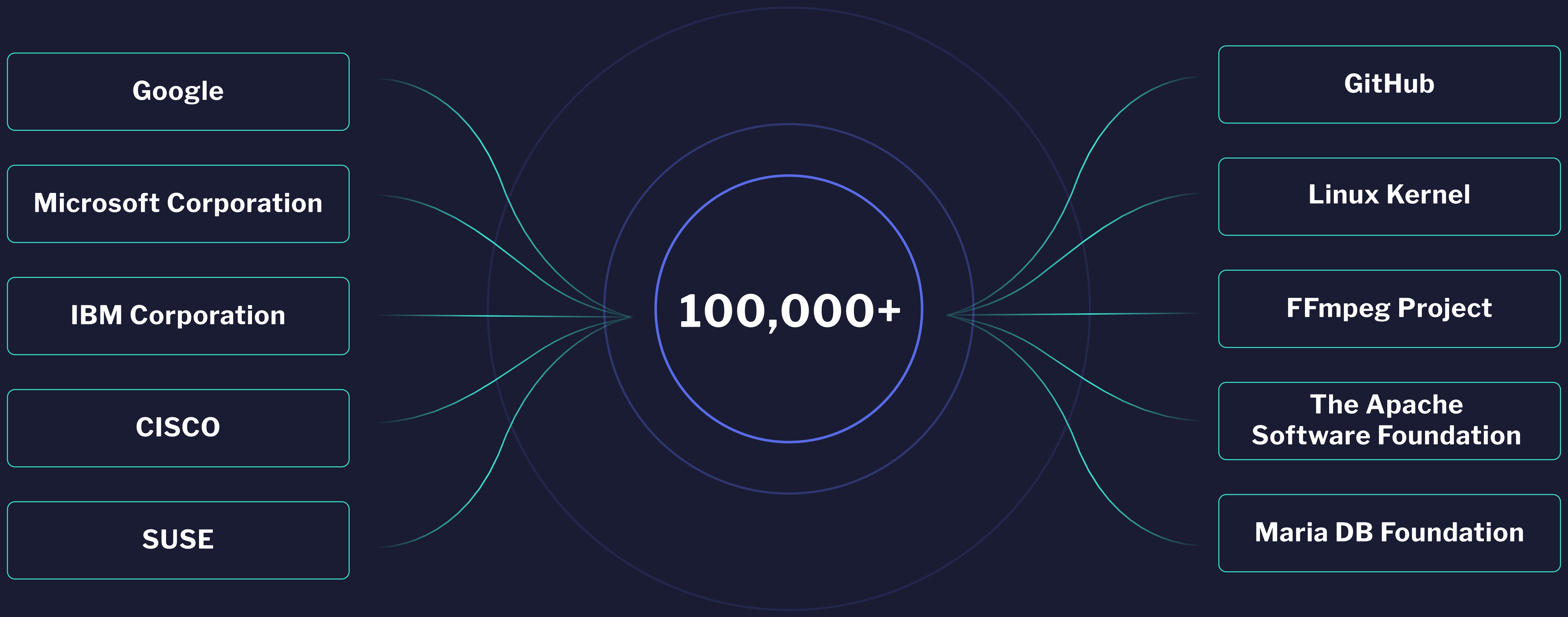
1. **Poor visibility and operational inefficiency:** Vulnerability Management Programs (VMP) strictly relying on CVE and NVD are likely unaware of nearly a third of all known vulnerability risk.

2. **Additional unknown, impactful risk:** Non-CVE vulnerabilities affect major vendors and well-known third-party libraries. In addition, more than half are high to critical in severity.

3. **Hidden threats in plain sight:** Threat actors have been using non-CVE zero-days and discovered-in-the-wild vulnerabilities in cyberattacks.

Additional unknown, impactful risk

Major Vendors and 3rd Party Libraries Affected by Non-CVE Vulnerabilities



Google

Microsoft Corporation

IBM Corporation

CISCO

SUSE

100,000+

GitHub

Linux Kernel

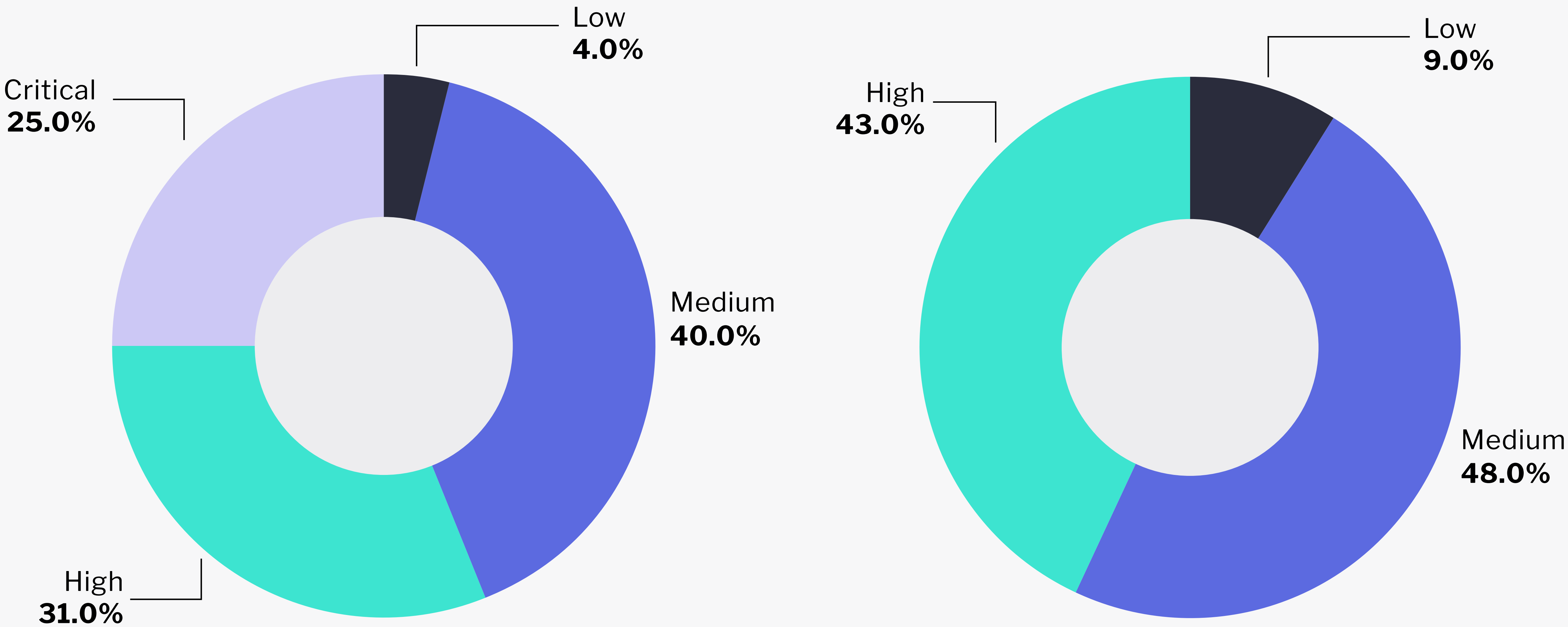
FFmpeg Project

The Apache Software Foundation

Maria DB Foundation

In addition, many of the missing vulnerabilities affect major vendors such as Microsoft, Google, Siemens, and more—impacting software that are used by most large companies. Many also affect well-known third-party libraries, which is a market historically underserved by CVE.

Breakdown of total non-CVE vulnerabilities by CVSSv2 and CVSSv3



According to CVSSv3, **56 percent** of the vulnerabilities missing from CVE are high to critical. Vulnerabilities with these severity scores are considered to pose a great risk to organizations and under most VMPs, are usually immediately prioritized for remediation. In addition, Flashpoint's non-CVE data accounts for **nearly a third** of all known disclosed remote and network access vulnerabilities.

CVSSv2

■	Low	**0.0 - 3.9**
■	Medium	**4.0 - 6.9**
■	High	**7.0 - 10.0**

CVSSv3

■	Low	**0.0 - 3.9**
■	Medium	**4.0 - 6.9**
■	High	**7.0 - 8.9**
■	Critical	**9.0 - 10.0**

FLASHPOINT

Hidden threats in plain sight

As of December 2023, CVE has documented over 740 instances of vulnerabilities being discovered-in-the-wild. However, Flashpoint's **VulnDB details an additional 40 percent** of documented in-the-wild vulnerabilities. Non-CVE vulnerabilities affecting major vendors and products fall within this subset.

Examples include:

- Adobe Reader
- Apple iOS
- Apple macOS
- Google Android
- Microsoft SQL Server
- MOVEit Transfer (DMZ)
- Siemens SIMATIC
- Solarwinds Orion Platform

The following have been exploited in some form of malware, yet do not have a CVE ID:

- Apache Hadoop
- Google Authenticator for Android
- PHP

FLASHPOINT

VulnDB: The most comprehensive source of vulnerability intelligence

Flashpoint's **VulnDB fully maps to CVE and NVD**, while providing better coverage and detail. Every entry, including issues missed by MITRE, is standardized and scrutinized, containing over 60 distinct classifications.

	VulnDB	CVE\NVD
Exploit details	✓	Limited
Attack location details	✓	Limited
Solution details	✓	Limited
Technical notes	✓	No
Affected product	✓	Limited
Affected versions	✓	Limited
Vendor & Product Risk Ratings	✓	No

Flashpoint goes above and beyond to provide customers with the most comprehensive, actionable, and timely source of vulnerability intelligence. On average, Flashpoint analysts are adding over 90 new vulnerabilities on average daily, while also updating hundreds of existing records. Using VulnDB's incredible level of detail, organizations can integrate non-CVE vulnerabilities into their existing workflows. **VulnDB can be leveraged in existing GRC, ITIL, CMDB, and many SIEM products.**

FLASHPOINT

ABOUT FLASHPOINT

Flashpoint is the pioneering leader in threat data and intelligence. We empower commercial enterprises and government agencies to decisively confront complex security challenges, reduce risk, and improve operational resilience amid fast-evolving threats. Through the Flashpoint Ignite platform, we deliver unparalleled depth, breadth and speed of data from highly relevant sources, enriched by human insights. Our solutions span cyber threat intelligence, vulnerability intelligence, geopolitical risk, physical security, fraud and brand protection. The result: our customers safeguard critical assets, avoid financial loss, and protect lives.

Discover more at **flashpoint.io**.