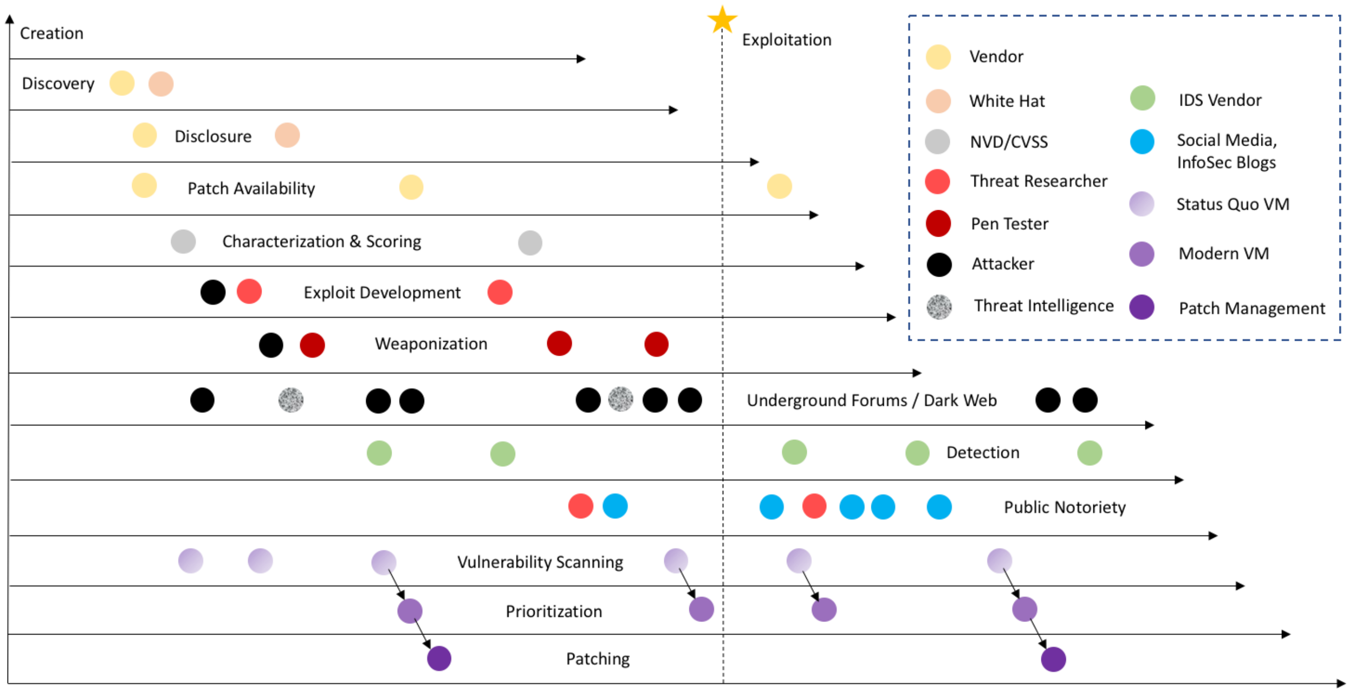
Balbix®



Creation

Discovery

Disclosure

Patch Availability

Characterization & Scoring

Exploit Development

Weaponization

Underground Forums / Dark Web

Detection

Public Notoriety

Vulnerability Scanning

Prioritization

Patching

Exploitation

Vendor

White Hat

NVD/CVSS

Threat Researcher

Pen Tester

Attacker

Threat Intelligence

IDS Vendor

Social Media, InfoSec Blogs

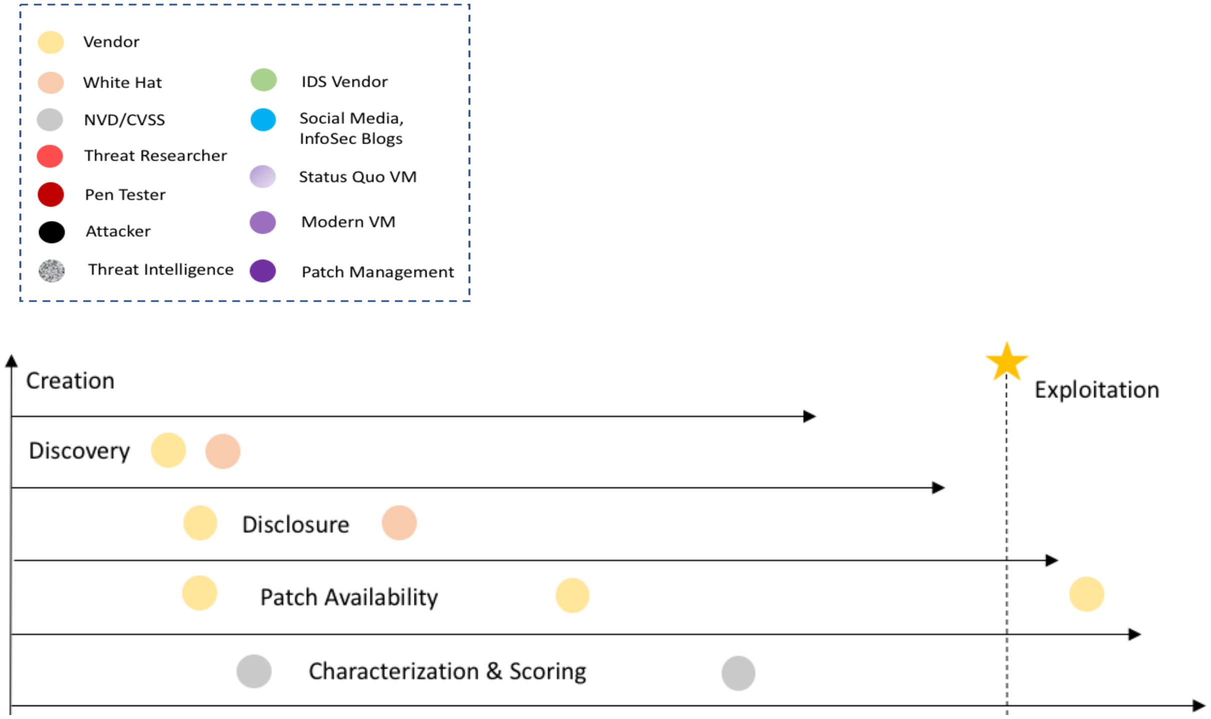
Status Quo VM

Modern VM

Patch Management

THE LIFECYCLE OF VULNERABILITY EXPLOITATION

From the time of introduction, the lifecycle of a single vulnerability goes through multiple stages involving several key stakeholders who each have different motivations and roles. Here we discuss the lifecycle and stakeholders with a particular focus on challenges at each stage.



1. DISCOVERY AND DISCLOSURE

The MITRE Corporation and the US National Vulnerability Database (NVD) have formalized the coordinated public disclosure of vulnerabilities. Once disclosed, vulnerabilities are given a name and made available as Common Vulnerabilities and Exposures (CVEs).

To date, about 120,000 CVEs have been made available through the NVD. Alternate sources are maintained by major software developers such as Microsoft (MS Bulletin), Oracle and Adobe, the Chinese government (CNNVD), Linux distributions, and private integrators.

THE CHALLENGE:

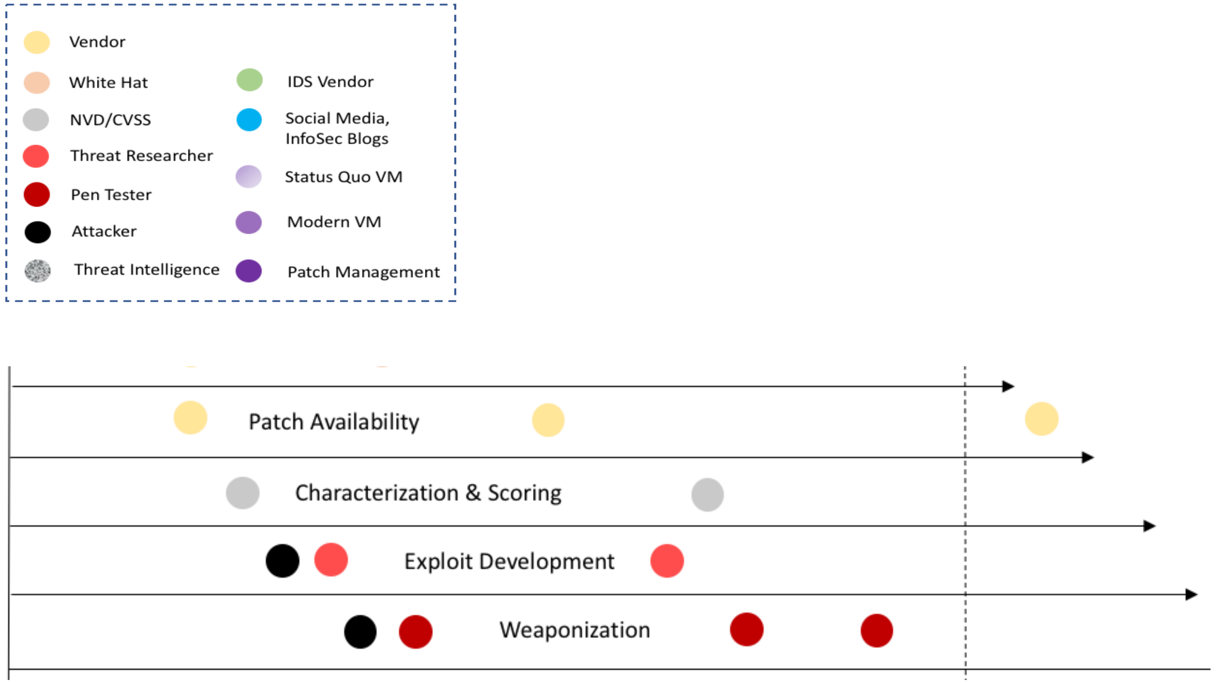
Lack of coordinated disclosure, high-quality curation, and centralized access to vulnerability definitions makes it hard for vulnerability management practitioners to scan their environment and identify which vulnerabilities are present.

2. PATCH AVAILABILITY

After a security patch is developed, vendors disclose the vulnerability and make the patch generally available. However, in typical scenarios, disclosure occurs through a third party, and sometimes, without a patch.

THE CHALLENGE:

This is a long-tail problem, with the majority of vulnerabilities addressed by a minority of vendors and it requires a nontrivial effort to discover and apply relevant patches for vulnerable software.



3. CHARACTERIZATION AND SCORING

CVEs are characterized and scored using popular open industry standards like Common Vulnerability Scoring System (CVSS).

THE CHALLENGE:

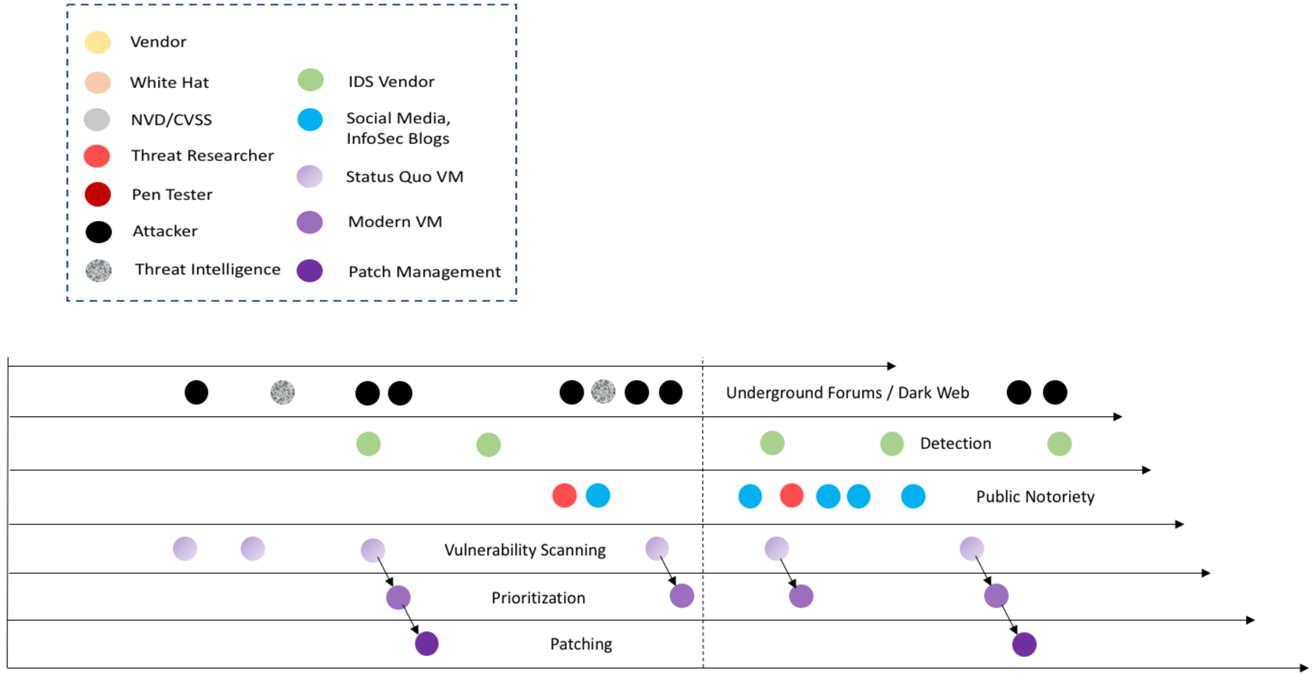
While the CVSS score has become the most used metric to prioritize vulnerabilities for remediation however, too many high or critical CVEs makes it difficult to tell the relative urgency of one from the other, leading to the need for further axes of prioritization. Prioritizing based on CVSS scores is not enough.

4. PUBLIC EXPLOIT DEVELOPMENT AND WEAPONIZATION

Exploit methodologies are developed by reverse-engineering patches. POC exploit codes are then developed and shared in the public domain, curated by databases such as Exploit DB.

THE CHALLENGE:

Unfortunately, exploit development and weaponization also occurs in the attacker community, so prioritization based on the stage of exploit development i.e., no exploit available to weaponize, is critical.



5. ATTACK MARKETS AND THREAT INTELLIGENCE

For CVEs with unknown exploits, attackers can develop and trade exploits in underground markets enabled by the dark web.

THE CHALLENGE:

Use threat intelligence in the right way to deepen your understanding of which vulnerabilities are most likely to be exploited in the current zeitgeist for your organization's size and industry vertical.

6. DETECTION OF EXPLOITATION IN THE WILD

Successful exploitation in the wild fuels attacker attention towards the vulnerability through public media and underground forums.

THE CHALLENGE:

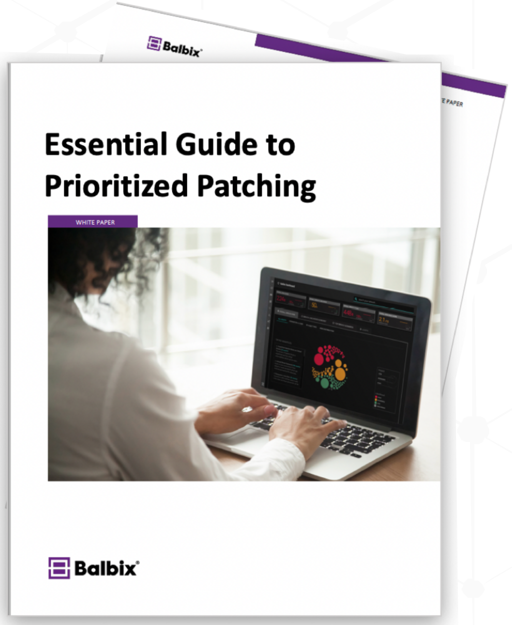
Understanding which exploits have been detected in the wild is important, however detecting such exploits depends on IDS signatures, which are prone to false negatives.

Balbix®

ADDRESSING THE CHALLENGES

Legacy vulnerability and patching tools use primitive risk metrics to prioritize vulnerabilities. Their calculation is typically based on CVE scores and a simple business impact model (high, medium, low), and leads to priority inversion and wasted effort.

Balbix's risk-based prioritization of vulnerabilities factors in vulnerability severity, threat level, business criticality, exposure/usage and the risk-negating effect of compensating controls. This results in very accurate prioritization and helps you avoid needless work on low priority issues.



Essential Guide to Prioritized Patching

WHITE PAPER

Balbix

Download the White Paper

www.Balbix.com