

Published (or Known) Vulnerability Analysis (PVA)

Executive Overview

Internet security researchers are continuously discovering critical attacks (exploits). Most exploits are derivative in nature and are related to other exploits, based on some common vulnerability. Signature-based security enforcement devices exist to selectively block any traffic flow matching a signature representing an attack, so there is an ongoing need to assess the effectiveness of these security enforcement devices. How can a user determine if a device equipped with given signature really blocks a traffic flow containing a given known vulnerability?

Despite the fact that new exploits appear virtually continuously, the rate of new underlying vulnerabilities is growing far more slowly than the rate of new exploits. It is not surprising that the vendors of these devices are transitioning to signatures based on vulnerabilities rather than exploits. This is beneficial for another reason: The performance of signature-matching engines suffers when large numbers of signatures are loaded. Basing such an engine on vulnerabilities means that a given signature can block many exploits, perhaps dozens. So, how can a vendor of these devices maintain their focus on building an accurate signature-matching engine based on vulnerabilities rather than exploits?

The Mu-4000 PVA subscription represents a methodical process that distills information about the most recently discovered, freshest root-cause vulnerabilities (those that have been discovered since 2004) into test cases that target the vulnerabilities behind tens of thousands of unique exploit vectors. Mu Dynamics' PVA subscribers can then audit their signature-based security enforcement devices to determine their exposure to the very latest underlying vulnerabilities.

Vulnerabilities, Exploits, Patches: Industry Trends

Pragmatic service providers and other end users have an ongoing need to balance between patching vulnerable end-systems, servers and network devices and using signatures to protect un-patched systems. Systems that are regularly patched should be vulnerable only to the very latest vulnerabilities that have appeared since the latest patch was applied. Once all systems have been patched (thereby eliminating a shared vulnerability), that signature is no longer needed. It is reasonable to expect that vulnerabilities from before 2004 are so old that vulnerable systems should have been patched by now. PVA offers a constantly updated subscription to ensure that perimeter defenses are effective, validated as protecting against the latest vulnerabilities that are affecting systems *today*.

Problems Solved by PVA

Despite the market transition toward vulnerability-based signature matching engines, there has been a lack of tools to validate the proper operation of these engines. When the Mu-4000 is equipped with a PVA subscription, networked security enforcement devices may be evaluated for their ability to block the latest vulnerabilities — so even when patches are not yet available for end-systems, users know that perimeter defenses are providing the expected protection. PVA ensures that the installed signatures actually work as expected.

- PVA enables customers to proactively quantify their risk to downtime or exposure to exploitable vulnerabilities and evaluate options for prevention before a fix is available for the vulnerable system.

Signature-based security enforcement devices are typically used to protect end-system, server, and networking platforms that are currently vulnerable but are as yet un-patched (the value of the signature evaporates once the vulnerable systems have been patched). Mu Security's PVA feature enables service providers and other end-users to verify that signature-based security enforcement devices are protecting the network in the window of time between when the vulnerability appears until the patch has been applied to the affected system.

- For those cases where the customer needs to selectively block the bad traffic but they lack a signature, some security enforcement products can create on-the-fly signatures from a packet capture, and so the Mu-4000 provides a sample PCAP for each PVA. Armed with this sample PCAP, customers can protect themselves in advance of an officially supported signature.
 - o The PVA subscription allows the user to ensure the on-the-fly (as well as the eventual “official”) patch’s efficacy at blocking the attack – before putting any patch into production. One should never presume that just because a signature is loaded that it is actually blocking the traffic associated with a known vulnerability or exploit. Trust but verify!

PVA Subscription Capabilities

PVA applies Mu Dynamics’ in-depth analysis in a timely fashion to a constantly growing list of published vulnerabilities (over 1000 dating back to 2004), updated as often as twice a month.

- The PVA subscription delivers tens of thousands of unique test cases. The thousands of supported vulnerabilities may be delivered over two different transports (i.e., IPv4 or IPv6), and these traffic streams may be transmitted through up to 12 different evasion techniques. Thus, each new vulnerability is multiplied into up to 24 new test cases.
- At the conclusion of any Mu-4000 PVA analysis, the user may generate a report itemizing blocked and missed attacks.
- Packet captures and detailed documentation are available for PVAs.
- PVA integrates into the Mu-4000’s regression framework, enabling users to re-run prior analyses with specific filters, including the ability to restrict a test to the set of published vulnerabilities that were available on the date of the original analysis.
- Establishing a quality or product vulnerability trend line is another PVA subscription benefit.

PVA Benefits

Signature-based security enforcement device vendors are using PVA to verify that new signatures are proven effective before shipping them to their customers, especially as they transition their products to focus on vulnerabilities rather than exploits. As the industry migrates toward vulnerability-based signatures, the Mu-4000 is the first test tool based on vulnerabilities (as opposed to exploits) and is uniquely positioned to facilitate this market transition.

FEATURE

BENEFITS

Up-to-date active attacks corresponding to published (known) vulnerabilities.	Service Providers obtain better information about if and how their systems are vulnerable, which helps them avoid downtime and minimize risks.
Integration with internal database for remediation and reporting.	Service Providers and end users can leverage the historical data for trend analysis including the ability to re-run old analysis exactly as they were done in the past. Users can also generate reports for data collected months or years ago.
Mutation analysis complements the usage of PVAs by mapping the attack surface of protocols involved in known attacks.	Service Providers can exercise the target protocol implementations with a “perfect storm” of crafted packets purpose-designed to expose software coding errors in protocol implementations that have not yet been discovered by hackers so they can insist on a fix from their vendor before it causes downtime or revenue loss.

Table-1.

IT departments and service providers own many tools designed to protect their network from various types of attack. However, the IT staff cannot deploy these defenses to best effect unless they have specific knowledge of whether or how their systems are vulnerable. Continuously auditing their network infrastructure using their Mu-4000’s PVA subscription raises awareness of the latest real vulnerabilities as soon as possible, so protective measures can be established until the end-systems have been patched to remove each vulnerability. Knowledge is power.

Armed with this knowledge, end-users at service providers and IT departments maximize uptime while minimizing the risk to their network, its users, and their data by ensuring that the protective gear that they already own is deployed for maximum effectiveness against the attacks that are relevant to their network now. For example, a Mu-4000 could verify weekly or daily perimeter defense “protection levels” against the most recently identified critical attacks. PVA delivers comprehensive “through and through” auditing of a complete chain of protective devices that comprises a typical “defense-in-depth” configuration.



web: www.mudynamics.com | email: info@mudynamics.com
 address: 686 W. Maude Ave., Suite 104, Sunnyvale, CA 94085, USA
 phone: (866) 276-4640 or (408) 329-6330 | fax: (408) 329-6317