Security Management System (SMS) v6.4.0
Threat Protection System (TPS) v6.4.0

December 16, 2024

Trend Micro is pleased to announce the release of TippingPoint OS v6.4.

This release is supported on all TippingPoint TX and TXE appliances, vTPS, vSMS, SMS H3, H4, and H5 standard and XL platforms.

This release includes the following enhancements:

◊ Easier TLS decryption using ACME to automate certificate management

Protecting your publicly addressable encrypted web services/services has just become even more efficient. By leveraging the ACME protocol, you can now fully automate:

- **Certificate Signing & Renewal:** automatically obtain a new certificate when needed.
- **Domain Validation:** automatically verify domain ownership without manual intervention.
- **Certificate Installation:** CA-signed certificates are automatically installed, allowing for simple, transparent inspection of TLS-encrypted traffic to the protected server.

This initial release leverages **Let's Encrypt Certificate Authority**, with additional CA's included in subsequent releases.

◊ Domain Reputation (formerly DNS Reputation) now acts on HTTPS traffic without requiring decryption.

Domain reputation can now be applied to encrypted HTTPS traffic without decrypting the payload (when the SNI field is transmitted in the clear). This is in addition to the existing domain reputation filtering capabilities, which apply to DNS and HTTP header traffic. HTTPS support is added to our existing support on DNS and HTTP and is operationally simple to deploy as no further configuration is required (*) when the SNI field is transmitted in the clear - no decrypt is needed.

◊ **Domain Reputation Enhancements - TLS handshake inspection**

Domain reputation filtering has been enhanced to support wildcards, allowing filtering by country code or top-level domains. This new enhancement can also be applied to domain names and geolocation filtering, which works by leveraging IP to Geo-mapping.

◊ **File Reputation**

This new capability enables users to filter suspicious objects by file hash, specifically SHA1 and SHA256. This initial version supports matching file hashes via HTTP (and HTTPS in conjunction with on-box TLS decryption or third-party TLS decryption device).

Support for file hash suspicious object submission matches the capabilities of other Domain, IP, and URL reputation features. Vision One can provide this manually via the SMS UI, SMS API, and STIX/TAXII.

◊ **Packet Trace included in Syslog Message.**

To improve scale and resilience, packet traces generated when a filter is matched can now be included as part of the syslog message output from SMS to an SIEM/collector. This can improve scale and help avoid challenges matching PCAP files with security events.

◊ **Other enhancements and fixes**

This release includes several other enhancements and fixes; for a complete list, please refer to the product Release Notes.

Thank you,
Trend Micro™ TippingPoint

For updated contact information, please click here.