Vectra Detect Platform Software Update

The Vectra® X-series appliances, B-series appliances, S-series sensors, VM and Cloud Brain, VM and Cloud Sensors, are scheduled to be updated to Vectra Detect for Network software release version 7.7. The Version 7.7 release updates OpenSSL to address a high CVE, updates our Beacon Detector coverage, adds some performance improvements to the Suspicious Admin and Smash and Grab Detections, faster detection reporting, M365 Log Disabling Coverage, and several bug fixes.

Release Schedule

7.7 will have the following release schedule:

- **Customers with Remote Support Enabled:** Customers who have remote support enabled will receive the update on or after May 8th, 2023
    - You can check if you have remote support enabled under Settings -> Services with Remote Support set to Enabled.
- **Customers Connected to Updater**: Customers who do not have remote support enabled but are connected to Updater will receive updates on or after May 15th, 2023
    - You can check if you are connected to Updater under Settings->Services and see that Updater Destination shows as connected, while Remote Support shows disabled.
- **All Other Customers***: Will be able to download the update on or after May 15th, 2023
    - *Note: This does not impact customers that have requested they be pinned to a specific release from support.

Platform

OpenSSL Update — Vectra Detect for Network

OpenSSL has been updated to address CVE-2023-0286, where an attacker could take advantage of a type confusion vulnerability relating to X.400 address processing inside an X.509 GeneralName to read memory contents or enact a denial of service.

For more information, please see CVE-2023-0286

Detections

Vectra constantly evaluates detection algorithm coverage and efficacy using opt-in metadata and direct user feedback, which drives targeted enhancements in our algorithms. We encourage your feedback via the Vectra user community.

Beacon Detector Update — Vectra Detect for Network

Version 7.7 provides an update to the Beacon Detector to detect more evasive C2 channels.

Algorithm Performance Improvements — Vectra Detect for Network

Vectra has made performance improvements to the Suspicious Admin and Smash and Grab Detections. There should not be any noticeable change in functionality, and no action required by the user, but the algorithms will perform better when the system is busy than previous releases.

HTTPS Proxy Traffic Handling Improvement — Vectra Detect for Network

Vectra has made an improvement when parsing proxy traffic which switches from HTTP to HTTPS within a single connection. This enhancement improves detection efficacy and protocol attribution in proxy environments. Some customers may notice an uptick in HTTPS Hidden Tunnel Detections in the 7.7 release. For more information about this change, please see: https://support.vectra.ai/s/article/KB-VS-1644

Faster Detection Reporting — Vectra Detect for M365 and Detect for Azure AD

Several Vectra M365 and Azure AD detections have been enhanced to report threats within less than an hour of Vectra receiving and processing the relevant logs from Microsoft. Specifically, Azure AD MFA-Failed Suspicious Sign-On, Azure AD Suspected Compromised Access, Azure AD Suspicious Sign-on, Azure AD Change to Trusted IP Configuration, Azure AD Privilege Operation Anomaly, M365 Malware Stage: Upload, M365, Suspect Power Automate Activity, and M365 DLL Hijacking Activity, M365 Risky Exchange Operation and M365 Suspicious Sharing Activity.

M365 Log Disabling Coverage — Vectra Detect for M365 and Detect for Azure AD

Expanded coverage for when an attacker attempts to disable logging from an Azure AD and M365 tenant.

Bug Fixes

CS-6025: AD context missing from Account pages when primary AD fails

Addresses an issue where account pages do not show AD context information when configured to use a secondary AD URI/IP if the primary AD server becomes unreachable.

CS-7649: Long running Brain backup may cause sensors replication alerts

Addresses an issue where long running brain backups may stop services for an extended period causing sensor replication alerts due to metadata buffering once the services are restarted.

CS-7548: Threat Intel show out-to-in traffic as in-to-out

Addresses an issue where the Threat Intelligence detection incorrectly shows out-to-in traffic as in-to-out.

CS-7675: M365 sensor detail incorrectly shows Anonymize Sensitive Data setting

Addresses an issue where sensor detail show the Anonymize Sensitive Data setting as disabled even when the setting is enabled.

CS-5883: Failed to test Kafka error

Addresses an issue where testing Kafka configuration may show “Failed to test Kafka configuration” even when logs are flowing correctly.

CS-7609: VHE hostname incorrectly shown as “192” in syslog

Addresses an issue where VHE hostname may be shown as “192” in syslog messages. This patch will set VHE hostnames in syslog to the serial number of the appliance.

CS-5883: Failed to test Kafka error

Addresses an issue where testing Kafka configuration may show “Failed to test Kafka configuration” even when logs are flowing correctly.

CS-7656: Group creation from Account page results in “Invalid members”

Addresses an issue where an “Invalid members” error is shown when trying to add members as part of the group creation process on an account page.

CS-7312: Missing artifacts due to delayed processing

Addresses an issue where artifact processing was delayed, resulting in missing artifacts.

CS-7808: Increase in Hidden HTTPS Detections after the 7.6 release

This issue is temporarily expected after the 7.6 and 7.7 releases. For more information please see: https://support.vectra.ai/s/article/KB-VS-1644

Appendix:

Will this upgrade perform a reboot of the Brain or Sensors?

No reboot is required as part of the 7.7 update.