CLAROTY

Continuous Threat Detection (CTD) Release Notes

CTD Version 4.6.2

21-Sept-2022

To view the most updated version of this document, visit docs.claroty.com

1. What's New?

Version 4.6.2 of Claroty's Continuous Threat Detection (CTD) provides significant new features and enhancements as follows:

Table 1. CTD V4.6.2 New Features and Enhancements

New Feature or Enhancement	Description
Improved Data Transfer Integrity	The improved CTD polling mechanism now ensures that data transfer via the CTD REST API is successful despite sync problems due to performance issues or server downtime.
Improved TDS Protocol Performance	The TDS protocol was refactored for faster performance.
Enhanced Database Performance	To improve database and overall system performance, Alerts are now saved in the database for one year from the time of occurrence. This change does not affect Asset visibility or any other part of the system.

2. Resolved Issues

The following table details issues resolved in V4.6.2 of Continuous Threat Detection (CTD).

Table 2. Resolved Issues

ID	Related Case ID	Area	Description
RNEW-20356		Active Discovery	Active Query fails if an asset does not have an IP address.
RES-2627	16176	Active Discovery	SNMP Network Layout query fails to generate file when using "@" symbol in community.
RES-2623	15709	Active Discovery	Some assets have IP records with octets that are in reverse order e.g. 111.88.13.120, 120.13.88.111.
RES-2586	14678	Active Discovery	CrowdStrike query fails when files do not have unique names.
RES-2585	14678	Active Discovery	The CrowdStrike Query fails parsing TIA projects that are archived - zip/zap files.
RNEW-20493		Active Discovery	Random invalid data occurs.
RNEW-20505		Active Discovery	When an exception occurs on a sensor, Active Tasks continue to run.
RNEW-20185		Activities	Users with Visibility > Manage RBAC permissions are able to edit Zones.
RNEW-20183		Activities	In Zone Rules, duplicating multiple rules is permitted, causing an error.
RNEW-20182		Activities	In a downloaded or exported Activity Log, the time format should be the same as all other reports.
RNEW-20181		Activities	Filters selected in the OT Audit page for a scheduled report do not appear in the report's row in the Report page.
RNEW-20208		Alerts	In the Threat Detection Overview, clicking the Open Stories number (in the top info bar) opens the Alerts page showing Alerts instead of Stories.
RNEW-19969	13997	Alerts	Alert list differs on Site and EMC.
RNEW-20436	16259	Alerts	In the Layered Topology view of Assets, filters are not applied.
RNEW-20366	16005	Alerts	Cannot change the size of the Alerts PCAP folder in Settings > Management > General > System Configuration tab.
RNEW-20148		Alerts	In the Alerts page, when deleting default filters and adding new ones, the default filters still appear after refreshing the page.
RNEW-18747		Alerts	Error occurs when attempting to resolve a New Conflict Asset alert.
RNEW-20496	16315	Alerts	When resolving Alerts, applying filter criteria and selecting the "Select all" checkbox causes all alerts to be resolved instead of only those meeting the filter criteria.
RES-2584		AppDB	AppDB does not correctly parse Mitsubishi GX Developer project files for PLCs that contain built-in Ethernet ports.

ID	Related Case ID	Area	Description
RNEW-19106	13687	Asset Management	Cannot delete a network despite its assets being deleted.
RNEW-12957	8931	Asset Management	In the Assets page, cannot select a different Preset if one has already been applied.
RNEW-20435	16297	Backup and Restore	Restoring from CTD UI or CLI fails.
RNEW-20400	16074	Backup and Restore	Scheduled backups stop working after first backup.
RNEW-20187	11646	Baselines	In Alert View page > Baseline Details for Alert table, the Last Seen date is earlier than the First Seen date.
RNEW-20072	15314	Concluder	Unresolved alerts are missing event details.
RNEW-20361		Integrations	CTD/FortiGate Integration - Not all Zone Rules get to FortiGate firewall.
RNEW-20288		Policies	Validated rules are replaced by unvalidated ones.
RNEW-20316		Reports, Tables	Pagination is missing in the Reports table - when the number of reports exceeds the default (20), only the first table appears.
RNEW-20440		Rules and policies	Unable to move to next page in Zone Rules.
RNEW-20248	9663	Syslog	When creating a new Syslog Baseline message that uses the TLS protocol, if a server certificate file is uploaded, it does not appear to be saved the next time the message is opened.
RNEW-20011		Threat Detection	Threat Bundle status shows as Updated even on disconnected Sites.
RNEW-20232	15685	UI	Korean characters do not display correctly in Reports.
RNEW-16372	10544	UI	In the Asset Details page, resizing the page in the browser causes the Network Communication Map widget to display incorrectly,
RNEW-20240	12717	Visibility	Changing PLC mode does not consistently trigger an Asset Information Change alert
RNEW-20472	16046	Vulnerabilities	Full match CVEs still appear on a fully patched Windows host
RNEW-20142	15318	Widgets	A Widget created from the Alerts page using the Group By > Created (days ago) filter does not correctly filter the data in the Alerts page when clicked.
RNEW-20074		Widgets	The Info Bar widgets cannot be removed when creating custom views of Overview pages.
RNEW-20391	16088	Work from EMC	In the EMC, cannot move from the Alert View page to any other page after clicking a Policy Violation alert.
RNEW-20501		Work from EMC	Active Query parameters defined directly on a Site are missing when updated from the EMC.

3. Known Issues

The following table details known issues in 4.6.2 of Continuous Threat Detection (CTD).

Item	ID	Area	Description
1.	RNEW-15410	Active Discovery	"Active Detection" item missing from the EMC Main Menu when active detection is enabled for a Site via the CLI.
2.	RNEW-15179	Alerts	If you assign Alerts to Users while logged directly onto a Site, the Alerts do not appear to be assigned when you view them from the EMC. (The Assigned To column is empty).
3.	RNEW-14427	Integrations	New sites connected to the EMC won't send updates about old assets.
4.	RNEW-16014	OS Configuration	Settings > Management > OS Configuration does not load when port forwarding and a non-standard port (not 443) is used
5.	RNEW-15666	Permissions	No results are displayed when a User in a Group with permissions defined per Asset/Zone opens the following pages: OT Audit, Baseline Summary, Protocol Summary, Network Sessions, DNS, Zone Rules. Also, the Threat Detection Overview might contain empty widgets for this Group.
6.	RNEW-16561	Related Alerts	Previous filtering applied in the Alerts page remains when the page is opened from Assets > Show Related Alerts.
7.	RNEW-18771	Rules	Alert rule filters might not auto-resolve for known-threat type alerts.
8.	RNEW-15455	Single entity page, Tables, Visibility	Vlan0 shows as "N/A" in the VLAN column of the Assets page, and does not display on the Detailed Asset page.
9.	RNEW-13859	Subnets	Settings > Management > Subnets - Wrong user name shown when editing a subnet tag.
10.	RNEW-18314	Widgets	For a customized Visibility Overview, the Asset Count Bar widget might get swapped out for one from the Enterprise Overview when upgrading CTD.