FortiEDR – Version 4.2.2.93 – Release Notes

Revision 1, May 2021

Last update: March 3, 2022

Resolved Issues

Central Manager 4.2.2.93

- **When logged in with Admin MSSP user data from the default organization is sometimes displayed rather than the selected organization data [Bug ID: 0758297]**
- **Rest API Collector sorting by lastSeenTime does not work as expected [Bug ID: 0776704]**
- **Playbook page loads slowly when there are many Playbook Policies to display [Bug ID: 781345]**

Central Manager 4.2.2.92

- **Wrong total number of Collectors shown on Inventory page in hoster view of multi-tenant setups [Bug ID: 764440]**
- **Expired Collectors are not calculated properly which results in wrong license seats calculation [Bug ID: 769249, 760511, 768620]**
- **Security events reclassified after being handled [Bug ID: 763047]**
- **MITRE tag links do not work for some of the rules [Bug ID: 770200]**
- **Low disk space alerts due to keeping redundant configurations [Bug ID: 770756]**
- **Managed devices with multiple mac addresses are displayed as unmanaged [Bug ID: 757709]**
- **System events on failed Collector registration following tenant migration [Bug ID: 773051]**
- **Devices are displayed as unmanaged although there is a Collector installed [Bug ID: 761119]**
- **Collectors become degraded due to missing configuration [Bug ID: 777272]**
- **Central Manager high CPU due to a deadlock in IoT handling [Bug ID: 768182]**
- **Central Manager fails to restart when LDAP configuration is corrupted [Bug ID: 772081]**
- **Icons are missing for toolbars in the Events Viewer page [Bug ID: 0785112]**
- **The Playbooks page loads very slowly when there are dozens of Playbook Policies [Bug ID: 781345]**

Central Manager 4.2.2.84

- **Collector registration fails when it is allocated with the same ID of a deleted Collector [Bug IDs: 769232, 766168]**
- **Central Manager is inaccessible when running full configuration in an environment with lots of exceptions [Bug ID: 769854]**
- **Dynamic content exceptions that are added from UI is being corrupted and also corrupts other existing dynamic content exceptions [Bug IDs: 732704, 743386, 761384]**
- **Central Manager console slowness due to long Exception icon calculation [Bug ID: 754696]**
- **IoT license seat calculation is wrong [Bug ID: 763127]**
- **Slow free-text search on the Events page [Bug ID: 772501, 767850, 766885]**
- **Internal DB failure when deleting applications [Bug ID: 772545]**

Central Manager 4.2.2.76

- **Opening the inventory tab takes minutes [Bug ID: 751035]**

- **Opening the Exception Manager takes a lot of time [Bug ID: 751954]**
- **Aggregator crashes every few days due to events bursts which also cause FCS to display as degraded [Bug ID: 0752771]**
- **Performance degraded related to network interface on organizations with no IOT [Bug ID: 751034]**
- **Communication control decision was created on a wrong group of collectors [Bug ID: 0743454, 0747067]**
- **Improve performance by calculating Exception icon only on expanded events of the Events UI [Bug ID: 0754696]**
- **Central Manager console slowness due to DB rollbacks in scenarios such as: IoT deep scans, failed (VDI) Collectors registrations due to long group name or long comm control query [Bug ID: 754817, 754457, 757020]**
- **Console login using SAML is not working due to Central Manager deadlock [Bug ID: 0755671]**
- **Playbook actions do not take place or are delayed when Playbook action to move to a high-security group is set [Bug ID: 0752441, 0753300]**
- **Application vulnerabilities are not learned when the affected OS or description fields are too long [Bug ID: 0752020]**
- **Collectors become degraded due to cut configuration [Bug ID: 0760537]**
- **Applications might not load correctly in case they are detected on more than 32K Collectors [Bug ID: 757020]**
- **Central Manager console slowness due to corrupted applications arriving from Core [Bug ID: 0752980, 0748696]**
- **Audit log for deleting events contains wrong data [Bug ID: 0755210, 0757497]**
- **Events advanced search window opens up very slowly due to OS calculation for dropdown [Bug ID: 0748696]**
- **Resolved applications keep coming back as unresolved communication control applications [Bug ID: 0748420]**
- **Console slowness that is related to DB locks done when there are Collectors registrations [Bug ID: 0748696]**
- **Improve events learning efficiency by removing a global lastEventTime update [Bug ID: 0762466]**
- **New VDI Collector is registered but stays as disconnected [Bug ID: 0766168]**
- **Collectors or Cores become disconnected/degraded due to failure in creating full configuration [Bug ID: 0767494, 0766484, 0760266, 0766707, 0762466, 0763979]**
- **Cannot disable or enable a Collector that is running on Hyper V from the Inventory page [Bug ID: 0760039]**
- **Central Manager console is very slow to respond due to OOM [Bug ID: 0763329, 0767494, 0765276]**
- **Slow console due to DB rollback when applications and CVEs are learned at the same time [Bug ID: 761440, 0766873, 0763979, 0767890, 0765991]**
- **Inconsistent system events behavior that is related to Collector status change [Bug ID: 0743248]**
- **Slow console due to inefficient processing of playbook actions [Bug ID: 0764855]**
- **Event tab indicator count is wrong since it considers old events that are not displayed [Bug ID: 0754659]**
- **Slow upgrade from V4 to V5 on setups with many registered Collectors [756305]**

Central Manager 4.2.2.58

- **Collectors cannot connect to Aggregator due to an empty configuration, following tenant consolidation [FortiEDR internal: EN-55064]**
- **Central Manager fails to start due to wrong Connector configuration, following tenant consolidation [FortiEDR internal: EN-56446]**
- **Collector cannot register to Aggregator due to slow registration process [FortiEDR internal: EN-57884]**

- **Device is still showing as unmanaged although it was installed with a Collector [FortiEDR internal: EN-57367]**
- **Deleting Collectors and tenants can take a very long time [FortiEDR internal: EN-60137]**
- **Search for Collectors last seen on Inventory works well only for part of the Collector Groups [FortiEDR internal: EN-60139]**
- **Improve Collectors registration [FortiEDR internal: EN-57129, EN-55075]**
- **Collectors/Cores registrations and status reports get stuck [FortiEDR internal: EN-57926, EN-65931]**
- **Collectors cannot register to Aggregator due to slow registration process [FortiEDR internal: EN-57884]**
- **Error uploading content with outdated MacOS installers - v3.1 for pre-Big-Sur devices [FortiEDR internal; EN-51519, EN-56451]**
- **Core never registered to Aggregator following first deployment [FortiEDR internal: EN-59032, EN-59500]**
- **New events are not consumed following software exception [FortiEDR internal: EN-59282]**
- **Event emails are not sent due to NPE [FortiEDR internal: EN-59556]**
- **Slow DB queries due to connection to DB not being properly closed [FortiEDR internal: EN-60082]**
- **Sluggish performance when loading large Events or Forensics [FortiEDR internal: EN-60052]**
- **Manager fails to start due to incorrect LDAP/SAML settings [FortiEDR internal: EN-57883]**
- **Manager fails to consume events and apps for a long-time causing Core to become degraded and a delay in events processing [FortiEDR internal: EN-60128]**
- **OOM in management due to progress bar that is never cleaned [FortiEDR internal: EN-60602]**
- **Delayed events processing due to starvation caused by a noisy event/Collector [FortiEDR internal: EN-50181]**
- **Central Manager slowness due to repeated FCS handling of the same event [FortiEDR internal: EN-61031]**
- **An exception seems to not apply due to slow event processing while displaying coverage in UI [FortiEDR internal: EN-61178]**
- **Network discovery wrongly marks devices with existing Collectors as unmanaged devices and makes duplications of IOT devices [FortiEDR internal: EN-58210, EN-54585]**
- **Events displayed with future time [FortiEDR internal: EN-61171, 0730832]**
- **Block duplicate events RDIs to reduce manager load [FortiEDR internal: EN-62334, EN-63788]**
- **Failure in sending events emails due to short SMTP connection timeout [FortiEDR internal: EN-62359]**
- **Collector status not displayed correctly due to no retries upon Aggregator failures to send it to Central Manager [FortiEDR internal: EN-61168]**
- **Many Collectors report disconnected because wrong port is in use with custom collector installer [FortiEDR internal: EN-64433]**
- **Collectors displayed as disconnected on Central Manager although they are running [FortiEDR internal: EN-65245]**
- **Error when creating communication control policy rule with many vendors [FortiEDR internal: EN-65286, 0741617]**
- **Failed to export Exceptions report [FortiEDR internal: EN-39442]**
- **Protection widget displays wrong protection coverage data [FortiEDR internal: EN-65618]**
- **Do not send configurations for two separated Aggregators simultaneously [FortiEDR internal: EN-65923]**
- **Failed to process event due to type bit error [FortiEDR internal: EN-66506]**
- **Email alerts are delayed [FortiEDR internal: EN-66688]**
- **Manager OOM due to Rest API authentication token that is never released [FortiEDR internal: EN-66605]**
- **An Exception cannot be set on listen events due to missing destination address [FortiEDR internal: EN-59134]**
- **GUI extremely slow when searching or loading exceptions windows due to applications with invalid property field [FortiEDR internal: EN-66659]**

- **New applications are not showing up on Communication Control when there is a burst of applications learning [FortiEDR internal: EN-66611]**
- **IOT devices are not discovered across multiple subnets [FortiEDR internal: EN-65793]**
- **Searching numeric values on Events page while in device view yields an error [FortiEDR internal: EN-63084]**

Central Manager 4.2.2.23

- **Add degraded reasons for non-approved extensions or Full Disk Access with MacOS Collector v4.1 [FortiEDR internal: EN-39575]**
- **Allow filtering out Collector degraded reasons, such as the one for failed OTI [FortiEDR internal: EN-54778]**
- **Security events are not sent from Aggregator to manager when HttpClient is stuck [FortiEDR internal: EN-54744]**
- **Communicating applications do not populate communication control and/or application usage is missing [FortiEDR internal: EN-52867, EN-52868]**
- **Exceptions cannot be set when path ends with a space because it is trimmed [FortiEDR internal: EN-50365]**
- **License count discrepancies related to wrong determination of server/desktop Windows devices [FortiEDR internal: EN-50970]**
- **Reports generation fails when done with an LDAP user [FortiEDR internal: EN-50183]**
- **Cannot pull Manager and Aggregator logs [FortiEDR internal: EN-53251]**
- **Dashboard events discrepancy due to device control events considered in dashboard graphs by mistake [FortiEDR internal: EN-51404]**
- **System events are not marked as read [FortiEDR internal: EN-51388]**
- **Process path wrongly displays subdirectory as the server name in case of network folder as the process mount point [FortiEDR internal: EN-52075]**
- **Collectors degraded following an upgrade from the Central Manager [FortiEDR internal: EN-55043]**
- **Core or other components may seem disconnected although up and running [FortiEDR internal: EN-54731]**
- **Assigning connector to a playbook action fails [FortiEDR internal: EN-53132]**
- **Registered collectors are not reflected in console [FortiEDR internal: EN-50149]**
- **High CPU on Aggregator and no configuration available [FortiEDR internal: EN-51966, EN-52222]**
- **UI is sluggish or stuck or no events populating on massive DB access [FortiEDR internal: EN-50887, EN-53312, EN-53321]**
- **NPE related to Communication Control Application usage [FortiEDR internal: EN-54142]**
- **Memory issues when generating report with a large number of events [FortiEDR internal: EN-50369]**
- **Remote operations such as disable/enable Collector stop working after a while [FortiEDR internal: EN-50969]**
- **OS selection dropdown on Inventory advanced search is very slow [FortiEDR internal: EN-48161]**
- **Central Manager slow down [FortiEDR internal: EN-50150]**

Central Manager 4.2.2.10

- **File scan doesn't kick off due to wrong configuration sent from Manager to Collectors [FortiEDR internal: EN-48815, EN-48595]**
- **Cannot scroll down to see all Collector Group assignments to security policies [FortiEDR internal: EN-39242]**
- **Events Excel report is corrupted[FortiEDR internal: EN-33473]**
- **Rest API new or update event do not update events comments [FortiEDR internal: EN-44193]**

- **Repeated FCS comments are not added to event handling comments [FortiEDR internal: EN-48983]**
- **Organization export and import fails due to an error related to users [FortiEDR internal: EN-43773]**
- **Errors when deleting an event while FCS reclassification occurs[FortiEDR internal: EN-20539]**
- **Organization deletion takes few minutes to complete [FortiEDR internal: EN-47374]**
- **Collectors usage information on Communication Control applications is wrong [FortiEDR internal: EN-21009]**
- **Applications are not being learned if the connection is coming from the same device in some cases [FortiEDR internal: EN-49630]**
- **Communication Control - Applications export report fails when Vendor filter is applied [FortiEDR internal: EN-48677]**
- **Slow responses on Central Manager Console due to missing indexes [FortiEDR internal: EN-44659]**
- **Manager is running out of disk space since mem dump files are not being cleaned [FortiEDR internal: EN-45439]**
- **Devices not shown on the Central Manager console after registration [FortiEDR internal: EN-48600]**
- **Disabling Collector fails when internal limits for remote operations are reached [FortiEDR internal: EN-46672]**
- **Error processing events due to integer/long mixup [FortiEDR Connect: EN-48222]**
- **Rest operations cause DB connection exhaustion such that Cores are disconnected [FortiEDR internal: EN-41941]**
- **Manager becomes slow and requires restart [FortiEDR internal: EN-44658]**
- **Marking tens of thousands of events as read at once gets stuck [FortiEDR internal: EN-44417]**
- **Aggregator drops events caused by integer overflow [FortiEDR internal: EN-45186]**

Central Manager 4.2.0.146, Core 4.2.0.139:

- **Aggregator get stuck when events flood pushes system limits [FortiEDR internal: EN-42904]**
- **Central Manager resources exhausted when there are hundreds of thousands events on navigation tabs bubbles [FortiEDR internal: EN-43683]**
- **UI actions are not completed due to Rest API operation that got stuck [FortiEDR internal: EN-41491]**
- **Allow using IP only in on premise multiple Aggregator installations [FortiEDR internal: 42162]**
- **Policy assignment to Collector Groups fails [FortiEDR internal: EN-42205]**
- **Device Control Events are displayed under the un-handled Events filter [FortiEDR internal: EN-30183]**
- **Fix failures on Organization migration [FortiEDR internal: EN-44195]**
- **Allow Collectors to migrate to new environment when source environment's license is expired [FortiEDR internal: EN-43595]**

Central Manager 4.2.0.138:

- **Fix Aggregator load balancing in setups with multiple Aggregators [FortiEDR internal: EN-39938]**
- **Improved Aggregator performance achieved with limiting HttpServerVerticle [FortiEDR internal: EN-41230]**
- **Improved performance by limiting the number of concurrent Collectors registrations [FortiEDR internal: EN-41250]**
- **Improved performance by more efficient handling of Collectors registration attempts to tenants with an expired license [FortiEDR internal: EN-41233]**

Central Manager 4.2.0.137:

- **Improve configuration generation [FortiEDR internal: EN-35114, EN-37145, EN-35997]**

- **Improve Collector registration flow [FortiEDR internal: EN- 34995, EN- 35255]**
- **Improve Communication Control and Dashboard queries and updates performance [FortiEDR internal: EN-36093, EN-36094, EN-35265]**
- **Improve Central Manager memory usage by separating installers from full configuration [FortiEDR internal: EN- 36752]**
- **Reduce load on manager by ignoring events from unregistered collectors [FortiEDR internal: EN-27330]**
- **Remove empty groups from full configuration [FortiEDR internal: EN-19984]**
- **Collectors are not upgraded from Central Manager due to empty installers [FortiEDR internal: EN-39267]**
- **In a multi Aggregator setup all Cores become disconnected due to same DNS value in use [FortiEDR internal: EN-34218]**
- **LDAP authentication fails with Central Manager v4.2 [FortiEDR internal: EN-36952]**
- **Cannot manually handle or archive events when ECS response handling malfunctions [FortiEDR internal: EN-28547]**
- **Get logs operation times out frequently [FortiEDR internal: EN-35742]**
- **Update Events (PUT) API request with a comment overrides previous comments [FortiEDR internal: EN-35065]**
- **Fix VirusTotal link [FortiEDR internal:EN- 34530]**
- **IoT - cannot select Collector Groups to exclude on IoT settings section [FortiEDR internal: EN- 32938]**

Core 4.2.0.137:

- **Improve events sending from Core to Aggregator [FortiEDR internal: EN-31210]**

Core 4.2.0.132:

- **Memory corruption in Core [FortiEDR internal: EN-34173]**
- **Improved performance by applying more efficient events re-sending to Aggregator in case of faliures [FortiEDR internal: EN-38387, EN-32392, EN-32390]**
- **Core crash when receiving device control event from an old Collector [FortiEDR internal: EN-32029]**
- **Powershell event doesn't display script on exception due to incorrect parsing [FortiEDR internal: EN-32591]**

Known Issues

- **Component Backwards Compatibility –** V4.2 Central Manager supports Cores/Collectors from older versions with limited functionality. Some new features introduced in later versions may not be available.
- **Upgrading from Older Versions –** A direct upgrade path for backend components (Central Manager, Aggregator, Core, Threat Hunting Repository) from V3.1 or earlier is not supported.

  Workaround to resolve this issue –

  - Upgrade the older environment to V4.0 or V4.1 before upgrading it to V4.2.
- **Collector May Fail to Install or Upgrade on Old Windows 7 and Server 2008 Devices That Cannot Decrypt Strong Ciphers with Which FortiEDR Collector is Signed –**

  Workaround to resolve this issue –

  - Patch Windows with Microsoft KB that introduces SHA-256 code sign support.
- **Some AV Products, Including Windows Defender and Some Versions of FortiClient, Require Disabling Their Realtime Protection in Order to be Installed Alongside FortiEDR Collector –**

This is a result of FortiEDR registration as an AV in the Microsoft Security Center that was introduced in V4.0. Although there is no need for more than a single AV product installed on a device, FortiEDR can be smoothly installed even if there is another AV already running. However, there are some other products whose installation fails if there are other AV products already registered.

Workaround to resolve this issue –

- Disable realtime protection on the other product or remove FortiEDR's AV registration with Microsoft Security Center

- **SAML Authentication Fails When Username on Identify Provider is Identical to Local User's –**

  Workaround to resolve this issue –

  Delete the local FortiEDR users that have usernames identical to ones on the SAML identity provider. Create other, different local users, if needed.

- **Number of Destinations Under Communication Control is Limited to 100 IP Addresses.**

  Isolation mode takes effect only on new trials to establish a network sessions following isolation mode initiation. Connections that have been established prior to device isolation, would remain intact. Same applies on Communication Control denial configuration changes.

  Both Isolation mode and Communication Control denial do not apply on incoming RDP connections and ICMP connections

- **Limited Support When Accessing the Manager Console with Internet Explorer or EdgeHTML –** Chromium Edge is supported as well as Chrome, FireFox and Safari 11 and above.

- **Newly Created API User Cannot Connect to the System Via the API.**

  Workaround to resolve this issue –

  - Before sending API commands, a new user with the API role should log into the system at least once to set the user's password.

- **Interoperability with AVG –** When AVG is installed on the device, it blocks the Collector connection.

  Workaround to resolve this issue –

  - Set exceptions in AVG on the FortiEDR Collector.

- **Downgrading the Collector Version –** When downgrading and restarting a device, the Collector does not start.

  Workaround to resolve this issue –

  - Uninstall the Collector, reboot the device and then install the older version.