FortiEDR – Version 5.0.2 – Release Notes

May 2021

Last update: October 25th 2021

Version Highlights

- **XDR** – Leveraging the Fortinet Security Fabric, FortiXDR delivers fully automated, extended threat detection, investigation and response in order to make thing easier for the IT security staff. FortiXDR utilizes FCS (Fortinet Cloud Services) advanced analytics, artificial intelligence and a predefined response framework in order to identify cyberattacks in progress – before they become data breaches or ransomware incidents.
- **Event Advanced Analysis View** – Incident response and forensic actions are detailed in an advanced analysis view listing the automated steps conducted during the event analysis process by FCS.
- **Threat Hunting** – New advanced and extensive behavior-based threat hunting, with embedded MITRE techniques and the support of process-based threat hunting of files, registry keys, event log and network related activities. The new threat hunting capabilities include granular collection policies and collection exclusions for better control of the magnitude of the collected data.
- **Scheduled Queries** – Scheduled threat hunting queries to enable customized rulesets based on audited collected behavior.
- **Web Filtering** – Automatic web filtering powered by the FortiGuard intelligence service.
- **Security Events Exceptions Enhancements** – Several exception enhancements, such as user-based exceptions, that lower Total Cost of Ownership (TCO) with FortiEDR.
- **Extended Linux Support** – The FortiEDR Collector is now supporting Oracle Linux OL (formerly OEL), in addition to the currently supported distributions: Red Hat Enterprise Linux, CentOS and Ubuntu.
- **Enhanced End User Notification** – User tray notification now provides visibility into recent events, as well as into Collectors' versions and states.
- **Control Windows Security Center Registration** – The FortiEDR can now be set as the threat protection solution from the Central Manager console.
- **Rest API Additions** –
  - Threat Hunting queries and settings.
  - Events API has been enriched with malware details and recommended remediation details.
  - Unmanaged devices list.
  - SAML SSO configuration.
  - Refer to the *FortiEDR API Guide V5.0* for more details.

Resolved Issues

Central Manager – Build 281

- The status of Collectors is not presented properly in the Central Manager (Collector registration issue) [0736622, 0750448, 0736844, 0746869, 0740781, 0734262, 0737226, 0736691, 0736469]
- Events are triggered although an Exception that is based on IP Set exists [744863, 0736085, 0739078, 0743513, 0743961, 0738141]
- There was sluggish performance when loading large Events or Forensics [735767, 741141]
- FCS was shown as Degraded following an Aggregator malfunction [0752771]
- The destination address was missing in Listen events [0734582]
- Email alerts were delayed [0734785, 0744420, 0748220]
- Playbook actions did not take place or were delayed when a Playbook action to move to a high-security group was set [0752441, 0753300]
- The deletion of a security event failed in an environment that had numerous events [743387]

- The editing of an exception failed if the underlying Event had been deleted [753486]
- The Inventory tab and the Exception Manager tab took a few minutes to open [751035, 751954]
- The export of the Exceptions report failed [FortiEDR internal: EN-39442, 0734622]
- The File Scan of a target Collector group that included more than 20k Collectors failed [**743881**]
- A proper reason for the degradation of a Collector is not presented when it is because of a driver verifier [738047]

Central Manager – Initial 5.0.2 Build

- There was sluggish performance when loading large Events or Forensics [FortiEDR internal: 735767, 741141]
- Playbook actions did not take place or were delayed when a Playbook action was set to move a device to a high-security group [FortiEDR internal: 0752441, 0753300]
- Some UI actions failed, such as assigning a connector to a playbook or accessing the Exclusion Manager [FortiEDR internal: EN-53132]
- The Events Excel report was corrupted [FortiEDR internal: EN-33473]
- Report generation failed when performed using an LDAP user [FortiEDR internal: EN-50183]
- The integration connector test failed when it was triggered by a local Admin user [FortiEDR internal: EN-51569]
- Local Admins in an MT environment could not set Exclusions [FortiEDR internal: EN-50260]

Known Issues

- **Component Backward Compatibility –** V5.0 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 V4.1 or earlier is not supported.

  Workaround to resolve this issue – Upgrade the older environment to V4.2 before upgrading it to V5.0
- **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 antivirus (AV) in the Microsoft Security Center that was introduced in V4.0. Although there is no need for more than a single AV product to be 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 when 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, now also available via UI.
- **SAML Authentication can fail when used with Azure SSO due to exceeded time skew –**

  Workaround to resolve this issue – Sign out and then sign in again to Azure so that the date and time provided to FortiEDR are refreshed.
- **Number of Destinations Under Communication Control is Limited to 100 IP Addresses.**
- **Limited Support When Accessing the Manager Console with Internet Explorer, EdgeHTML and Safari 13 or above –** Chromium Edge is supported as well as Chrome, FireFox and Safari 11 and above.
- **Safari 11.1 on MacOS Malfunction Upon Events Viewing**
- **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 in order to set the user's password.
- **Isolation and Communication Control connection denial are not supported with Oracle Linux Collectors.**
- **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.