FortiEDR – Version 4.1.1 – Release Notes

Revision 1, April 2020

Version Highlights

- **Fortinet Look and Feel –** The enSilo platform is now named FortiEDR with a complete Fortinet look and feel.
- **Internet of Things (IoT) Security** – Reduce the attack surface by providing complete visibility into which IoT devices are connected to the enterprise network in order to minimize exposure to security risks on these devices that can propagate to other devices in the organization. Devices are classified by type (printer, media devices, network devices and so on) and are listed on the FortiEDR console with details, such as geo-location and internal IP, so that they can be identified and managed as needed.
- **Detect Rogue Devices** – Detect workstations and servers in the organizational network that are not protected with FortiEDR Collector. Such unmanaged devices should be installed with a Collector so that they do not pose a risk to other assets in the network or alternatively, should be moved to another less-strict VLAN (for example, *guest*).
- **Extended Orchestration with Enhanced Fabric Integration** – Using built-in connectors, FortiEDR leverages Fortinet Security Fabric to extend its automatic Playbook actions to include, among other responses, block malicious IPs by FortiGate and move compromised devices to different subnets by FortiNAC. Moreover, FortiSandbox can now be easily integrated with FortiEDR, leveraging its capabilities for analyzing specific files before they are executed.
- **Easier FortiNAC and FortiSIEM Integration** – The internal source IP is now included in syslog messages to enable easier integration with NACs and SIEMs.
- **Security Assertion Markup Language (SAML) Single Sign On (SSO) Authentication** – Logging in to the FortiEDR Console using any SAML 2.0 identify provider is now available.
- **Download Collector Installers from the Central Manager** – On the Central Manager console, select the Collector version of choice for Windows, MacOS or Linux and get a prepopulated custom Collector installer that can be silently deployed on your devices.
- **Improved License Control for Tenants in Multi-tenancy Setups** – Control which add-ons are included for each Organization – Vulnerability and IoT Management and/or Forensics and Threat Hunting.
- **Extended Device Information** – The exact operating system version and build were added to the console and reports. Hardware details, such as CPU, memory, motherboard, firmware and storage, as well as operating system details are now available with the list-collectors REST API.
- **Improved Collectors Installation Failure Detection –** Improved the detection of Collector failures upon new installation or upgrade in cases involving disk space shortage, a missing Windows KB or situations where the Collector-Aggregator connection is broken due to SSL interception by a proxy. In such cases, the Collector is displayed in a *Degraded* state on the console, with an indicative warning message.
- **Threat Hunting Repository Disk Space Management** – New system events were added when reaching capacity limits in order to allow for the archiving of old data and/or to add further storage.
- **New Rest API Actions –**
  - New APIs for IoT Management – create-iot-group, list-iot-groups, delete-devices, list-iot-devices, move-iot-devices and rescan-iot-device-details.
  - New APIs for Communication Control – list-policies, clone-policy, set-policy-rule-state, set-policy-permission and resolve-applications.
    Refer to the *FortiEDR RESTful API Guide V4.1* for more details.

Resolved Issues

- Allow deleting Collectors from multiple pages in the Inventory tab.
- Allow exporting an Executive Summary Report for a tenant in multi-tenancy setups.
- AV certification with Microsoft Security Center is supported also on Windows XP.

Known Issues

- **Component Backwards Compatibility –** V4.1 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 before upgrading it to V4.1.
- **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.**
- **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.