IT Operation Platform

February Release

2019/02/16

Table of Contents

Introduction **3**

Endpoint Manager **3**

Endpoint Manager Core 3

New Features 3

Improvements 3

Security 3

New Features 3

Improvements 4

Remote Tools 4

New Features 4

Improvements 4

Remote Monitoring and Management 5

New Features 5

Comodo Client Security **5**

Windows 5

New Features 5

Improvements 6

Linux 7

Improvements 7

Portal **7**

New Features 7

New Features 7

Improvements: 7

Service Desk **7**

New Features 7

Improvements 8

APPENDIX-1 **8**

Introduction

This document contains detailed notes about February 2019 release, scheduled to go live Saturday 2019/02/16. The release is expected to take 4 hours to deploy, during which time Comodo One will be in maintenance mode.

Endpoint Manager

Endpoint Manager Core

New Features

- TLS 1.2 Upgrade

To comply with the best industry security practices, we are upgrading the protocol used in our communication client (CC) to Transport Layer Security (TLS) 1.2.

You will need to make sure that the version of CC on your Windows (XP, 2003 Server, 7 and 2008 Server) devices is version 6.16.10680.18030 or higher before 07-01-2019 (July 1st 2019).
Here is the wiki of this feature.

Improvements

- Logged in User

Added the ability to see the user logged into a device in the 'Device List'. You can search, sort and filter according to this new field.

Bug Fixes

- Fixed the issue of upgrade button under license options section.
- Fixed the issue of phone numbers under support section for ITarian and Comodo ONE
- Fixed the issue of delayed application of profile settings to devices.
- Fixed the issue of role management for editing device name.
- Fixed the issue of high CPU usage for communication client.
- Fixed the issue of communication client proxy settings with symbol '\'.
- Fixed the issue of notifications which cannot be removed for Android devices.
- Fixed the issue of grey screen in Kiosk mode for Android devices.

Security

New Features

- Improved heuristic analysis and embedded code detection settings.

With this feature, interpreter interactions with suspicious autoruns items can be configured separately for each interpreter type. This means even better protection against malicious code triggered by Windows start-up and auto-run items. You can configure the feature in the new ‘Script Analysis’ section in Profiles.

Improvements

- New ‘Script Analysis’ section. ‘Heuristic Command Line Analysis’ and ‘Embedded Code Detection’ have been moved to the new script analysis section in a profile. This provides more granular management of security components.
    - General Settings. You can enable or disable the ‘Runtime Detection’ feature from this tab, and also limit the size of scripts which should be analyzed.
    - Runtime Detection. ‘Heuristic Command Line Analysis’ and ‘Embedded Code Detection’ settings have been moved to this section.
    - Autoruns Scan. Interpreter configuration for scanning/monitoring autorun items can be done from this section.
- Valkyrie details about a file can now be viewed in the ‘Security Dashboards’ area. Simply select a file in the security dashboards screens and click ‘Valkyrie details’.
- Download Valkyrie reports from the security dashboard. Simply select a file in the security dashboard and click ‘Valkyrie Report’ to view granular information about the file.
- Added a ‘Show ignored containment events’ filter in to the security dashboard. In ‘Event View’, you can now show all ignored containment events. We think you’ll find this addition useful, but please note that we disabled the new filter by default. This is a practical move to highlight more important activities and lessen the potential noise created by multiple ignore events.

Remote Tools

New Features

New additions to file explorer functionality. We know you’ve been looking for these and we’re excited to deliver!

- Upload files of any format to remote endpoints from your admin device (50MB file
  New remote folder operations:
  Here is the wiki for this feature
    - Create folders

    - Rename folders & files
    - Delete folders & files Here is the wiki for this feature

You can enable or disable folder operations for specific staff by configuring the user role (‘Users’ > ‘Role Management’).

Improvements

- More informative error messages in the file explorer interface allow you to troubleshoot and react to issues faster.

- Moved the info box that appears on an endpoint during remote connections to the bottom left corner of the screen. We expect this repositioning will improve user experience by freeing up desktop space.

Remote Control

Bug Fixes

- On some MAC endpoints, crashes observed and this caused connection initiation. The issue was identified and is fixed.

Remote Monitoring and Management

New Features

- **Network Management**

We are proud to announce the addition of a brand new section for network management. The first feature in the new section is ‘Network Discovery’, and we’ll be adding many more network capabilities in upcoming releases.

Network Discovery:

- Discover devices from the probe device you select
- Add new IP ranges for discovery
- Add exclusions for IP ranges
- Set SNMP v1.2 to discover network devices
- Get alerts and logs when items are discovered
- Easily view discovered devices in ‘Device List’ > ‘Discovered Devices’. Here is the wiki of this feature.

Improvements

- **Custom scripts failures for monitoring**
  With this release, custom scripts monitors could be setup by ability to select the trigger for script failures.

Bug Fixes

- Fixed the issue of high CPU consumption of monitors.
- Fixed the issue of repeating service crash of monitors for some customers.

Patch Management

Bug Fixes

- Software inventory was not showing the list of softwares and third party applications of patch management. This is fixed.

Comodo Client Security

Windows

New Features

- Prevent registry keys from being read by contained applications. You can now stop the virtualization of specific registry keys by the containment module. This will prevent unknown applications from reading potentially sensitive data held in those keys (write access is already disabled by default). You can access the setting in CCS at ‘Advanced Settings’ > ‘Containment’ > ‘Protected Objects’
- Option to disable real time scans on network items. Real time virus scans are now optional for items on shared network directories. This will improve system performance because, if an endpoint does not have the rights to delete or quarantine items in shared folders anyway, there is less reason to run real time scans on them. Network files that are copied to the endpoint will, of course, still be scanned and handled locally.
- Antimalware Scan Interface (AMSI) Integration. CCS now provides even better malware protection via our integration with Microsoft AMSI. This means deeper software scans and stronger protection for your endpoints. The option is disabled by

default, but can be enabled in ‘Advanced Settings’ > ‘AV Settings’ > ‘Real time scan’.

- Virtual Desktop. With this brand new component, you can virtualize your entire desktop and perform all tasks within a fully virtual environment. Everything!! Applications running in the virtual desktop are isolated from the rest of the endpoint, write to a virtual file system, and cannot access personal data. This makes it ideal for surfing the net without risk and even for testing out beta/unstable software. You can save any data you wish to keep to a special folder called ‘Shared Space’, which the host system can also access. You can launch the virtual desktop from CCS at Containment Tasks > Run Virtual Desktop. Go ahead and try it!

Admins can also set the following items for the virtual desktop:

- Password Protection. If enabled, password protection locks end-users in the virtual environment to stop them switching back to the host.
- Launch Virtual Desktop upon user login. Starts the virtual desktop automatically as soon as the endpoint is booted. Enable this setting in CCS at ‘Advanced Settings’ > ‘Containment’ > ‘Virtual Desktop’.

Improvements

- ‘Protected Objects’ are now under containment settings. ‘Protected Data’ and ‘Protected Keys’ have been moved to ‘Advanced Settings’ > ‘Containment’. This improves UI consistency by grouping these two items with related features and settings.

Bug Fixes

- The issue with firewall driver that causes connection problems is fixed.
- The issue with CCS Task Logs which was caused by spontaneous reboots during AV scans is fixed.
- The issue with applying profiles to CCS is fixed.
- The functionality issue with “jump folder” in scan window is fixed
- The issues that caused performance problems are fixed.

Linux

Improvements

- **TLS 1.2 Upgrade**

To comply with the best industry security practices, we are upgrading the protocol used in our security client to Transport Layer Security (TLS) 1.2.

Bug Fixes

- The issue with restoring quarantined items is fixed.
- The performance issue regarding to the compatibility with some specific browsers is fixed.

Portal

New Features

- You can now login to your Comodo One or ITarian account from any login page in the US or EU. We will redirect you to the correct region based on your account.

Improvements:

- It is now easier to remove plainPassword from the single sign-on (SSO) authentication process.

Bug Fixes

- Grammar issue has been fixed on the report.

Service Desk

New Features

- Added the ability to view device summaries direct from a ticket. Click on the device name in the ticket list or ticket detail and you can navigate to the device summary.
- Alerts for ticket stage changes. From now on you can receive email notifications when staff escalate a ticket to the next stage.

Improvements

- Reduced the amount of critical application errors
- Performance of ticket list has been improved.

- Weak password policy has been fixed.

Bug Fixes

- Workflow related notifications were not being sent.It has been fixed.

APPENDIX-1

New Client Versions:

- Endpoint Manager - Server version 6.26.22682.19020
- Windows Communication Client 6.26.22611.19020
- Windows Client - Security 11.1.0.7229
- Windows Remote Control 6.25.21754.19010
- macOS Communication Client 6.26.22671.19020
- macOS Client - Security 2.4.2.791
- macOS Remote Control 6.25.21758.19010
- iOS Mobile Agent 1.2.27
- Android Mobile Agent 6.13.5.11
- Linux Communication Client 6.25.21662.19010
- Linux Client - Security 2.2.1.400