Centero Software Manager supported application process

Last Modified

Centero Software Manager supported application process

This is a description of process for new Supported Application versions released by software vendors. This process is used with all the Supported Applications in CSM Services. In addition the same process is used for Application Packaging as a Service Apps (APaaS).

Monitoring for the new application versions and vulnerabilities

This part of the process consists of two simultaneous tasks.

- Centero's specialist goes through all the Supported Applications and APaaS applications daily. This means reviewing the sources of software vendors for any new versions available. The reviewing process includes all the different type of updates: security, quality, feature, bug fixes etc.
- In addition we have a background automation going through new software vulnerabilities every few hours. This is done with assist of Microsoft Defender for Endpoint, Advanced Hunt Queries and Microsoft Logic Apps.

New software version is detected

Whenever a new software version is detected Centero's specialist enters a record in our systems. At the same time the media of the new software version is introduced to our systems. This also means saving a SHA1 hash of the downloaded media to our systems. On top of that the specialist selects which kind of update is in question. This helps us to prioritize security updates over others for an example.

The SHA1 hash can be used at any later point of the process. It can be used for verifying that the media has not been altered by anything malicious.

When the specialist downloads the installation media of the new version for the first time, Defender for Endpoint also keeps track of the SHA1 hash and any possible changes to the hash.

Packaging specialist downloads the media

According to our packaging process a packaging specialist will start the work on the new version. This means downloading the media to an endpoint. Once again, Defender for Endpoint will scan and monitor the media. Microsoft Defender for Endpoint also uses Virus Total for signature based monitoring.

The packacing process starts

Centero Kapellimestarin Apulainen copies packaging project files to the endpoint of the specialist. These files also includes the media of the previous version. All the files are automatically scanned by Defender for Endpoint.

Differ[illegible]e new installation media

The me[illegible] is then either repackaged or modified. This part of the process requires differen[illegible] the metho[illegible]stEd anD PowerS[illegible]it.

The different methods the packaging specialist uses:

1. **Repackacing an EXE (.exe) executable file.** The specialist uses a fresh packaging virtual machine with Administudio Repackager to find out all the changes the executable does. All the necessary changes, files etc are then build into a new MSI-package. The finished installation media (.msi) is then tested on a fresh testing virtual machine.
2. **MSI package built by software vendor.** Whenever a software vendor already has a MSI-package available, then all the necessary changes are built into a MST-package. The MST package includes all the necessary configuration for the MSI-package. The finished installation media (.msi + .mst) is then tested on a fresh testing virtual machine.
3. **EXE files including a MSI or multiple MSI files.** The EXE file in extracted and then built into a single MSI package. All the necessary changes are built into a MST-package. The MST package includes all the necessary configuration for the MSI-package. The finished installation media (.msi + .mst) is then tested on a fresh testing virtual machine.
4. **EXE package released by software vendor.** On rare occasions an existing EXE-file is used. It is then tested on a fresh testing virtual machine.
5. **Using Powershell App Deployment Toolkit (PSADT).** PSADT is used to install either MSI or EXE package. Powershell script includes all the necessary configuration for EXE- or MSI-package.The finished installation media (script with .EXE or .MSI) is then tested on a fresh testing virtual machine.

Technical testing of the media for new software version

No matter what packaging method is used or what the type of the finished media is, the testing is always done on a fresh testing virtual machine. The tests include:

- Installation
- Removal
- Update

Publishing the new version for internal testing

The new version will be published by using our own utility tool Centero Kapellimestarin Apulainen. It means publishing the finished packages in format of .INTUNEWIN and .ZIP. The files are then scanned with Microsoft Defender. After that, all the necessary files are copied to Microsft Azure Storage.

Executing the internal tests

All the software versions are then tested by us. It includes the technical testing in earlier phase but also acceptance testing in the following management systems:

- M
- M
- M

We make sure that the new version is successfully imported to the management system and then delivered to testing endpoints.

Malware scanning

Before the final step of releasing the new media for customers we do extensive malware scans for the media. This is done with assistance of MetaDefender. MetaDefender includes multiple different anti malware engines.

If the scan is successful and no abnormalities are reported we proceed with the publishing process. If there is anything anomalous it is reported to the security team which will determine the what happens next.

Publishing to customers

This is the final part of the process. We used our our own utility tool Centero Kapellimestarin Apulainen to make the final publish for all our customers.

Assets used in the process

- Centero Kapellimestarin Apulainen utility tool
- AdminStudio Repackager
- AdminStudio InstallShield
- InstEd
- PowerShell App Deployment Toolkit
- Host machine
- Fresh Virtual Machine for Packaging
- Fresh Virtual Machine for Testing