Legacy products startup issue

2020-02-10 - Steef | ESET Nederland - Comments (0) - Customer Advisories

UPDATE 10-02-2020 11:20

Added more affected products

UPDATE 10-02-2020 17:20

Added solution, binary file fix

UPDATE 11-02-2020 15:00

Added affected products, addes Certfix.rar and changed download location and powershell script.

UPDATE 12-02-2020 09:00

Adjusted script command with logging.

UPDATE 12-02-2020 16:00

Added Module update information

UPDATE 13-02-2020 09:00

Updated CertFix - enhanced list of supported product versions (Feb 13, 2020) , Download links for ESET Endpoint Antivirus/ ESET Endpoint Security 5.0.2272.7

UPDATE 13-02-2020 20:30

New version of CertFix.exe, The fixing tool for v5

Alert Details

We would like to inform you that we have identified an issue in **older versions** of the product of our Windows business products, specifically:

ESET Endpoint Antivirus/ESET Endpoint Security 5	ESET Endpoint Antivirus/ESET Endpoint Security 6.5.2000+	ESET File Security for Windows 6.5.2000+	ESET Mail Security for Microsoft Exchange Server 6.5
5.0.2248.0	6.5.2086.0	6.5.12002.1	6.5.10057
5.0.2254.0	6.5.2086.1	6.5.12002.0	6.5.10059
5.0.2254.1	6.5.2093.1	6.5.12004.0	
5.0.2254.1000	6.5.2094.0	6.5.12007.0	
5.0.2260.0	6.5.2094.1	6.5.12010.0	
5.0.2260.1	6.5.2107.0	6.5.12013.0	
5.0.2265.0	6.5.2107.1	6.5.12014.0	
5.0.2265.1	6.5.2118.0	6.5.12017.0	
	6.5.2118.1	6.5.12018.0	
	6.5.2118.2		
	6.5.2118.3		
	6.5.2118.4		
	6.5.2123.5		

ESET Endpoint Antivirus/ESET Endpoint Security 5	ESET Endpoint Antivirus/ESET Endpoint Security 6.5.2000+	ESET File Security for Windows 6.5.2000+	ESET Mail Security for Microsoft Exchange Server 6.5
	6.5.2123.7 6.5.2123.8 6.5.2132.1 6.5.2132.2		

- **ESET Security for Kerio 6.5**
- **ESET Mail Security for Domino 6.5**
- **ESET Security for Sharepoint Server 6.5**.

This issue DOES NOT affect the latest versions of our products including the latestESET Endpoint Antivirus / ESET Endpoint Security- 6.6.2089 and ESET File Security for Windows 7.1.12018 and customers using the latest versions are not affected in any way. This issue relevant to the impacted versions is listed and described below.

ESET has identified that our kernel has a problem with verification of the timestamp of an already expired certificate (*expired by 7th Feb 2020*). This method fails and our modules in older, legacy versions, are declared as untrusted and therefore are not loaded. This mechanism ensures that no untrusted library is loaded.

As a result, the affected versions fail to load modules (Firewall, HIPS, Updated, Device Control, Web and Email protection) and are not functional, therefore the protection is not functional.

Newest versions of our products are NOT affected.

Symptoms:

For versions older than 5.0.2271.x symptoms are:

- Failed loading of modules for v5 family
- GUI of the main window is in English and logo shows ESET Smart Security 5 instead of Endpoint Security

For versions 6.5.x symptoms are:

- Product reports antiphishing as disabled
- Product reports that it is not activated
- Product's advanced settings have features missing

If they are managed by our ESET Remote Administrator or ESET Security Management Center, they will fall back to the respective parametric group and report an alert as not being activated and the antiphishing module as not functional.

Solution



Important!
If you are using affected versions and issue is not manifesting, **do not restart the machine** and perform upgrade immediately.

Frequently Asked Questions

Please read the following ESET Knowledgebase article: Legacy products startup issue FAQ

The following solutions are available:

1. If you have not restarted your computer with ESET Endpoint product yet, make sure you have **Update Module** (version 1074.2 for v6.5) and **Antivirus and antispyware module update** (version 1559.4 for v5) listed in Installed components. This modules ensures protection and allows for subsequent upgrade to the latest versions, which is required step to fully mitigate the situation.

Then upgrade to the latest version:

Install ESET Endpoint Antivirus 5.0.2272.7 or ESET Endpoint Security 5.0.2272.7
Install or upgrade ESET Endpoint Security or ESET Endpoint Antivirus on a client workstation (7.x)
Install and activate ESET File Security for Microsoft Windows Server (7.x)
Install ESET Mail Security for Microsoft Windows Exchange Server (7.x)
Install ESET Mail Security for Lotus Domino 7.1
Install and activate ESET Security for Microsoft SharePoint Server (7.x)

How to check the version of installed modules in ESET Endpoint Security

In the main program window, navigate to **Help and support > About ESET Endpoint Security** and click **Installed components**.

Another module updates for affected versions of ESET products will be available as soon as possible.

2. If you have restarted your computer with ESET Endpoint product v6.5, use the **fixing tool** and upgrade to the latest version if possible.

How to download and use the fixing tool for v6.5

Download CertFix.exe. If you are unable to download an executable file with your browser, download CertFix.rar. The fixing tool can be run or downloaded to the machine and automatically executed from CMD.exe with the following script (the log will be created):

```
powershell -command "& {(New-Object
System.Net.WebClient).DownloadFile('http://help.eset.com/eset_tools/CertFix.exe',
'%temp%\CertFix.exe');(Start-process '%temp%\CertFix.exe' -NoNewWindow)}" >
C:\CertFix.log
```

or if managed remotely, as client task in **ESMC → Operating system → Run command**.

3. If you have restarted your computer with ESET Endpoint product 5.x, use the fixing tool. If you have successfully applied the fix tool, **ESET Endpoint Antivirus/ESET Endpoint Security 5.0.2272.7** (5.0.2271.3 for JPN) is installed on your computer and it is fully functional. Next step is to **upgrade from 5.0.2272.7 to the latest version ESET Endpoint Antivirus 7.2.2055.0 / ESET Endpoint Security 7.2.2055.0** or also available on the ESMC repository, if possible.

How to download the fixing tool for v5

Choose the language and the version of the fixing tool below:

English	eea_nt32_enu.exe	eea_nt64_enu.exe	ees_nt32_enu.exe	ees_nt64_enu.exe
Dutch	eea_nt32_nld.exe	eea_nt64_nld.exe	ees_nt32_nld.exe	ees_nt64_nld.exe

4. If you have ESET Endpoint product 6.5.x running on Windows XP, use the fixing tool for v6.5. Upgrade to ESET Endpoint Antivirus/ESET Endpoint Security 6.5.2132.5 that is compatible with Windows XP.

How to download and use the fixing tool for v6.5

Download CertFix.exe. If you are unable to download an executable file with your browser, download CertFix.rar. The fixing tool can be run or downloaded to the machine and automatically executed from CMD.exe with the following script (the log will be created):

```
powershell -command "& {(New-Object
System.Net.WebClient).DownloadFile('http://help.eset.com/eset_tools/CertFix.exe',
'%temp%\CertFix.exe');(Start-process '%temp%\CertFix.exe' -NoNewWindow)}" >
C:\CertFix.log
```

or if managed remotely, as client task in **ESMC → Operating system → Run command**.



NOTE:
Windows PowerShell comes installed by default in every Windows, starting with Windows 7 SP1 and Windows Server 2008 R2 SP1.

Important!

We recommend upgrading **ESET Endpoint Antivirus/ESET Endpoint Security 5** by uninstalling version 5 and

installing the latest version ESET Endpoint Antivirus/ESET Endpoint Security 7.2. If you want to run version 5 anyway, we recommend upgrading to version **5.0.2272.7** which is not affected.

Click the appropriate link for your system in the table below to download the ESET Endpoint Security or ESET Endpoint Antivirus installer file.
Which version (32-bit or 64-bit) of ESET endpoint products should I download?

Your license information (ESET-issued username and password) is required for authentication.
How do I receive a Username, Password, and License Key for my ESET business product?

ESET Endpoint Security	**64-bit**	**32-bit**
EES installer	Download ESET Endpoint Security	Download ESET Endpoint Security
ESET Endpoint Antivirus	**64-bit**	**32-bit**
EEA installer	Download ESET Endpoint Antivirus	Download ESET Endpoint Antivirus

We strongly suggest upgrading **ESET Endpoint Antivirus/ESET Endpoint Security 6.5** to the latest version of ESET Endpoint Antivirus/ESET Endpoint Security 7.2.

We recommend upgrading **Server products version 6.5** to the following versions:

ESET File Security for Windows 7.1

ESET Mail Security for Microsoft Exchange Server 7.1

ESET Mail Security for IBM Domino 7.1

ESET Security for Sharepoint Server 7.1

For **ESET Security for Kerio 6.5**, we are working on it and we will get it fixed as soon as possible.

If you are having any concerns or questions – or are unable to upgrade to the latest versions - do not hesitate to contact ESET support .