ESET Customer Advisory: Upgrades necessary to ensure continuous protection

2020-07-23 - Steef | ESET Nederland - Reacties (0) - Customer Advisories

ESET Customer Advisory: Upgrades necessary to ensure continuous protection

Summary

At ESET, customer security is our top priority. The latest ESET product versions include important changes that expand on ESET-developed protection technologies and make them compatible with future OS updates.

Due to changes in the Microsoft Windows OS including support for strong cryptography standards, ESET cannot guarantee that older product versions will offer full functionality on current Windows builds. ESET customers may need to upgrade to a Windows-supported version to continue receiving protection. Please read the details below to see if your product version or Operating System requires an upgrade.

Solution

ESET has prepared a comprehensive migration guide for each of the scenarios described below. You can find the guide at https://support.eset.com/en/end-of-life/.

Details

I. Upgrade of ESET security products to latest versions to support Windows 10 21H1

Windows 10 21H1 includes some under-the-hood changes and ESET products need to be updated to support these changes to run on this upcoming OS version. Therefore, it is necessary to upgrade your ESET products and infrastructure to the supported versions (Endpoint 7.3+, ESMC 7.2+, home 13.2+) prior to the Windows update. Only these versions will continue to be supported on Windows 10 21H1.

In addition to compatibility with future Windows builds, these new versions of ESET security products deliver many new security features, performance improvements, and resolutions to issues reported for previous product versions. The migration guide available above contains a detailed overview of the benefits of using the latest product version.

II. Upgrade of Windows OS to support SHA2 code signing

ESET Endpoint products v.6.6+, ESET products for Windows servers v.7+ and ESET products for home users v.10+ load product modules in native .dll format, which is handled by the OS itself. The code integrity and origin, which are crucial for security, are ensured by digital signatures that rely on secure cryptography standards.
The IT industry is gradually phasing the older SHA1 standard out, as it is no longer considered cryptographically secure. It is being replaced with SHA2. If your OS does not currently support SHA2, but an update from Microsoft is available (applies to Windows 7, Windows Server 2008, and Windows Server 2008 R2), you need to add SHA2 compatibility to your older OS using the steps from the following Microsoft article: https://support.microsoft.com/en-us/help/4474419/sha-2-code-signing-support-update.

The deadline for this update is set by the expiration date of Microsoft's intermediate certificate that signed ESET's code-signing certificate. Therefore the update needs to be done before the end of January 2021. ESET products will start to communicate this requirement as a Status message later this year.

OSes that are no longer supported by Microsoft—such as Windows XP, Windows Vista and Windows Server 2003—and thus can't be updated to support SHA2, may, according to the New End of Life policy, use legacy ESET product versions, which utilize proprietary modules in a .dat format and thus are not subject to OS code signing support (see paragraph IV. for details). The same applies to installations of Windows 7 that for some

serious reason can’t be updated to Service Pack 1.

III. Upgrade of ESET Security products due to cross-certificate expiration

One of the certificates used in ESET Security products is signed by a trusted certification authority that expires on April 15, 2021. Because the algorithm used is SHA1 (no longer considered cryptographically secure), the trust won’t be renewed and products with this certificate will no longer update their modules, including the detection engine.

This issue is not dependent on the version of Windows OS, nor the installed Windows Updates. Therefore, it is necessary to upgrade the affected ESET products to the latest available version; the products will start to communicate this requirement as a Status message later this year. A detailed list of the affected products and versions can be found in the online guide available above in the “Solution” section.

IV. New “End of Life” policy

As the cybercrime world is constantly evolving, security products developed years ago can’t offer an up-to-date level of protection and ESET can’t guarantee further support for some of them. The End of Life policy has been simplified to be transparent and easy to understand so that ESET customers can check which combinations of product and OS version they can use. Please check the corresponding knowledgebase document to see the current status of your installed product and ESET’s plans for its support, so that you can schedule the upgrades at your convenience.

Feedback & Support

If you have feedback or questions about this issue, please contact us using the ESET Security Forum, or via local ESET Technical Support.