Local privilege escalation vulnerability fixed in ESET products for Windows

2021-01-20 - Steef | ESET Nederland - Comments (0) - Customer Advisories

ESET Customer Advisory 2021-0001
January 18, 2021
Severity: Medium

Summary

ESET was made aware of a vulnerability in its consumer, business, and server products for the Windows platform that allows users with limited rights to write a file or rewrite contents of an existing one, without having permissions to do so when **ESET Self-defense was not active**. ESET prepared installers with the issue fixed. We recommend using the latest versions of the installers available to ensure maximal protection.

Details

ESET received a report stating that on a machine where an ESET product is being installed or upgraded, running on Windows operating system, it was possible to make changes in an ESET directory in a way that forced the product to write into files that would normally not be writable by the user, thus achieving privilege escalation.

This vulnerability emerged because during the installation process, protection is only being set up, thus self-defense is not yet fully active. Once the installation is finished and self-defense is activated, the attack is not possible anymore. Likewise, the attack is also possible in some other scenarios when self-defense is turned off.

Since the window of time, when self-defense is inactive during installation and upgrade, is narrow and it is difficult to control by an attacker, we believe that the chance of successfully exploiting this vulnerability is low.

Upgrades by means of Micro Program Component Update (uPCU) are not affected, standard PCU is affected. The already installed ESET security product is protected by the Self-defense mechanism, which is enabled by default.

The reserved CVE ID for this vulnerability is CVE-2020-26941.

To the best of our knowledge, there are no existing exploits in the wild that take advantage of this vulnerability.

Solution

ESET has prepared fixed installation packages to be used by our customers to install and upgrade ESET security products:

- ESET NOD32 Antivirus, ESET Internet Security and ESET Smart Security Premium 14.0
- ESET Endpoint Antivirus and ESET Endpoint Security 8.0
- ESET File Security for Microsoft Windows Server, ESET Mail Security for Microsoft Exchange Server, ESET Mail Security for IBM Domino and ESET Security for Microsoft SharePoint Server 7.3

We strongly recommend that customers use the latest ESET security product versions and keep their operating systems up-to-date.

Affected products

Installation of or upgrade to one of the following ESET security products is affected:

- ESET NOD32 Antivirus, ESET Internet Security, ESET Smart Security, ESET Smart Security Premium versions 13.2 and lower
- ESET Endpoint Antivirus, ESET Endpoint Security, ESET NOD32 Antivirus Business Edition, ESET Smart Security Business Edition versions 7.3 and lower
- ESET File Security for Microsoft Windows Server, ESET Mail Security for Microsoft Exchange Server, ESET Mail Security for IBM Domino, ESET Security for Kerio, ESET Security for Microsoft SharePoint Server versions 7.2 and lower

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.

Acknowledgment

ESET values the principles of responsible disclosure within the security industry and would like to express our thanks to Ilias Dimopoulos of RedyOps Research Labs who reported this issue.

Version log

Version 1.0 (January 18, 2021): Initial version of this document