Potential local privilege escalation vulnerability fixed

2020-04-27 - Steef | ESET Nederland - Comments (0) - Customer Advisories

Summary

ESET was made aware of a vulnerability in its consumer and business 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. ESET prepared a fix, which is being distributed by automatic product updates; no user interaction is required.

Details

On March 20, 2020 ESET received a report stating that on a machine with an affected ESET product installed, running on an affected Windows operating system, it was possible for a user with limited access rights to create hard links in some ESET directories and then force the product to write through these links into files that would normally not be write-able by the user, thus achieving privilege escalation.

This vulnerability only emerged because of the combination of already existing vulnerabilities in handling hard links inside the Microsoft Windows operating system and the way ESET products handled write operations in given directories. ESET remedied this by changing how write operations are handled in affected directories in all products.

Microsoft released security updates to cover the underlying vulnerability in the operating system, without which the above described attack scenario won't be possible; see the Affected products section below for details.

The reserved CVE ID for this vulnerability is CVE-2020-11446.

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

Solution

ESET prepared a fix, distributed automatically in Antivirus and Antispyware Module 1561. The module is being distributed via automatic product updates, so no user interaction is required. Distribution of the module started on March 31, 2020 at 10:40 CEST for customers using the pre-release update channel and on April 14, 2020 at 10:30 CEST for users using the regular update channel.

We strongly recommend that customers also apply security updates from Microsoft accessible from the links listed in Affected products section below.

Affected products

For a product to be affected, all the following conditions need to be met:

- Installed product is one of:
  - ESET NOD32 Antivirus, ESET Internet Security, ESET Smart Security, ESET Smart Security Premium
  - ESET Endpoint Antivirus, ESET Endpoint Security, ESET NOD32 Antivirus Business Edition, ESET Smart Security Business Edition
  - 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
- The product has Antivirus and Antispyware Module version from 1553 to 1560 installed (click here for instructions on how to check the module version)
- Windows operating system does not have the March 2020 Security updates installed; see following Microsoft advisories for details:
  https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0849
  https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0841

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0840
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0896

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.

Acknowledgement

ESET values the principles of responsible disclosure within the security industry and would like to express our thanks to Trần Văn Khang (aka Khang Kì Tổ) — Infiniti Team, VinCSS (the member of the Vingroup) who reported this issue.