ESET Customer Advisory: Local privilege escalation vulnerability fixed in ESET security products for Windows

2023-08-14 - Steef | ESET Nederland - Comments (0) - Customer Advisories

ESET Customer Advisory 2023-0008

August 11, 2023

Severity: Medium

Summary

A report of a local privilege escalation vulnerability was submitted to ESET by the Zero Day Initiative (ZDI). The vulnerability potentially allowed an attacker to misuse ESET's file operations during a module update to delete or move files without having proper permissions to do so.

ESET fixed the issue with HIPS support module 1463, which was distributed automatically to ESET customers along with Detection engine updates. No action stemming from this vulnerability report is required to be taken by our customers.

Details

The vulnerability allows a user logged on to the system to perform a privilege escalation attack, misusing the ESET GUI to plant malicious files required for the attack into specific folders and later misusing file operations performed by ESET's updater component to possibly delete or move any arbitrary file.

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

The CVE ID reserved for this vulnerability is CVE-2023-3160, with the following CVSS v3.1 score and vector:

7.8: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Solution

ESET released an update with HIPS support module 1463 to patch this vulnerability in already installed products, which was distributed automatically. The distribution of the module update started on June 26 for pre-release users, followed by batches for general public users from June 28, with a full release on July 5. See the instructions how to check the versions of the modules.

As already installed products are patched by the HIPS support module update, customers with an ESET product installed and regularly updated do not need to take any action stemming from this vulnerability report.

For new installations, we recommend using the latest installers downloaded from www.eset.com or the ESET repository.

Affected ESET products

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

Feedback & Support

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

Acknowledgment

ESET values the principles of coordinated disclosure within the security industry and would like to express our thanks to Trend Micro’s Zero Day Initiative team.

Version log

Version 1.0 (August 11, 2023): Initial version of this document