ESET Tech Center

ESET Customer Advisory: Link Following Local Privilege Escalation Vulnerability in Quarantine of ESET products for Windows fixed

2024-06-21 - Steef | ESET Nederland - Reacties (0) - Customer Advisories

ESET Customer Advisory 2024-0008
June 20, 2024
Severity: High

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 restore operation from quarantine, which had to be initiated by a user with administrative privileges. This would allow the attacker to perform an Arbitrary File Creation Local Privilege Escalation. ESET fixed the issue in the Antivirus and antispyware scanner module 1610, which was distributed automatically to ESET customers along with Detection engine updates. ESET customer action stemming from this vulnerability report is not required.

Details

The vulnerability would allow a user logged on to the system to perform a privilege escalation attack by planting malicious files required for the attack in specific folders and later misusing file operations initiated by a user with administrative privileges and performed by ESET's service to create or overwrite arbitrary files.

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

The CVE ID reserved for this vulnerability is CVE-2024-2003, with the CVSS v3.1 score 7.3 and the following CVSS vector: AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H

Solution

ESET released a fix for this vulnerability for installed products in the Antivirus and antispyware scanner module 1610, which was distributed and applied automatically. The distribution of the module update started on April 10, 2024, for pre-release users, followed by batches for users among the general public on April 17, 2024, and the full release on April 22, 2024. Verify the product modules.

The Antivirus and antispyware scanner module update patched existing installed products. Customers with a regularly updated ESET product do not need to take any action based on this vulnerability report.

For new installations, we recommend using the latest installers available on www.eset.comor the ESET repository.

Affected programs

- ESET NOD32 Antivirus, ESET Internet Security, ESET Smart Security Premium and ESET Security Ultimate
- ESET Small Business Security and ESET Safe Server
- ESET Endpoint Antivirus for Windows and ESET Endpoint Security for Windows

- ESET Server Security for Windows Server (formerly File Security for Microsoft Windows Server)
- ESET Mail Security for Microsoft Exchange Server
- ESET Mail Security for IBM Domino
- ESET Security for Microsoft SharePoint Server
- ESET File Security for Microsoft Azure

Note

ESET product versions that have reached End of Life are not listed.

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 coordinated disclosure within the security industry and would like to express our thanks to Nicholas Zubrisky (@NZubrisky) and Michael DePlante (@izobashi) of Trend Micro’s Zero Day Initiative.