ESET Customer Advisory: Arbitrary file deletion vulnerability in ESET product installers on Windows fixed

2025-07-09 - Steef | ESET Nederland - Comments (0) - Customer Advisories

ESET Customer Advisory 2025-0009

July 9, 2025

Severity: Medium

Summary

A report of an arbitrary file deletion vulnerability (and, in extension, local privilege escalation vulnerability) was submitted to ESET by Sheikh Rishad. The vulnerability potentially allowed an attacker to misuse the installation file of ESET security products on Windows to delete an arbitrary file without having the permissions to do so.

Details

Upon pre-creating the target installation directory and setting certain redirects, the vulnerability in the ESET security product installer allowed an attacker with an ability to execute low-privileged code on the target system to delete an arbitrary file, thus escalating their privileges.

ESET fixed this possible attack vector and prepared new builds of its products that are no longer susceptible to this vulnerability (refer to Solution below).

Please note that the vulnerability is present in the installation file, rather than the installed security product itself – therefore, no risk stemming from this vulnerability applies once the ESET security product is installed and running on the system.

The CVE ID reserved for this vulnerability is CVE-2025-5028, with the CVSS v4.0 score 6.8 and the following CVSS v4.0 vector:
AV:L/AC:L/AT:N/PR:L/UI:A/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N

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

Solution

ESET prepared fixed installation files of its security products, which are available in the Download section of www.eset.com or via ESET Repository as well.

- ESET NOD32 Antivirus, ESET Internet Security, ESET Smart Security Premium, ESET Security Ultimate 18.2.14.0 and later

- ESET Endpoint Antivirus for Windows and ESET Endpoint Security for Windows 12.0.2058.0, 11.1.2062.0 and later from the respective version family
- ESET Small Business Security and ESET Safe Server 18.2.14.0 and later

ESET also published the fixed ESET Package Installer to ESET PROTECT and ESET PROTECT On-prem, and therefore, both the Live Installer and All-in-one installer packages newly generated by customers in these consoles after July 2 and July 3, respectively, are no longer susceptible to this vulnerability.

Affected products and versions

- ESET NOD32 Antivirus, ESET Internet Security, ESET Smart Security Premium, ESET Security Ultimate 18.1.13.0 and earlier
- ESET Endpoint Antivirus for Windows and ESET Endpoint Security for Windows 12.0.2049.0, 11.1.2059.0 and earlier from the respective version family (.exe installers only, not .msi)
- ESET Small Business Security and ESET Safe Server 18.1.13.0 and earlier
- Live Installer and All-in-one installer packages generated in ESET PROTECT and ESET PROTECT On-prem consoles on or before July 2 and July 3, respectively

End of Life product versions
ESET product versions that no longer receive hotfixes according to the End of Life policy may not be listed.

Feedback & Support

If you have feedback or questions about this issue, 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 Sheikh Rishad.

Version log

Version 1.0 (July 9, 2025): Initial version of this document