ESET Customer Advisory: Use-after-free vulnerability in ESET security products for Linux fixed

2026-07-16 - Steef | ESET Nederland - Comments (0) - Customer Advisories

ESET Customer Advisory 2026-0012

July 15, 2026

Severity: Medium

Summary

ESET was made aware of a use-after-free vulnerability in its security products for Linux by Diego Mondéjar Fernández of SICE. The vulnerability potentially allowed an attacker to trigger kernel panic on the system. ESET mitigated this by preparing fixed versions of the affected products.

Details

On systems with the affected ESET products installed, an attacker could, under specific circumstances and with specific timing, cause the system to execute a long-running syscall, which would result in the access of memory pages that were no longer used by the product. This would immediately trigger a kernel panic and, thus, a denial-of-service condition on the system.

The reserved CVE ID for this vulnerability is CVE-2026-6424, the CVSS v4.0 score is 6.7, with the following vector: CVSS:4.0/AV:L/AC:L/AT:N/PR:H/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N

To the best of our knowledge, no exploits exist in the wild that target this vulnerability.

Solution

ESET prepared fixed builds of the affected products and recommends upgrading to these or scheduling the upgrades in the near future. The fixed builds are available to download from www.eset.com or via ESET Repository.

- ESET Endpoint Antivirus for Linux
    - version 13.2.3.0 and later
    - version 13.1.5.0 and later from the 13.1 version family
    - version 13.0.5.0 and later from the 13.0 version family
    - version 12.2.9.0. and later from the 12.2 version family
    - version 12.1.2.0 and later from the 12.1 version family
    - version 12.0.14.0 and later from the 12.0 version family

- ESET Server Security for Linux
    - version 13.2.53.0 and later
    - version 13.1.118.0 and later from the 13.1 version family
    - version 13.0.36.0 and later from the 13.0 version family
    - version 12.2.73.0 and later from the 12.2 version family
    - version 12.1.407.0 and later from the 12.1 version family
    - version 12.0.292.0 and later from the 12.0 version family

Affected ESET products

- ESET Endpoint Antivirus for Linux
    - version 13.1.3.0 and earlier from the 13.1 version family
    - version 13.0.3.0 and earlier from the 13.0 version family
    - version 12.2.8.0 and earlier from the 12.2 version family
    - version 12.1.1.0 and earlier from the 12.1 version family
    - version 12.0.13.0 and earlier from the 12.0 version family
- ESET Server Security for Linux
- version 13.1.116.0 and earlier from the 13.1 version family
- version 13.0.34.0 and earlier from the 13.0 version family
- version 12.2.72.0 and earlier from the 12.2 version family
- version 12.1.406.0 and earlier from the 12.1 version family
- version 12.0.287.0 and earlier from the 12.0 version family

Note

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 Diego Mondéjar Fernández of SICE.

Version log

Version 1.0 (July 15, 2026): Initial version of this document