[CA8230] Use-after-free vulnerability fixed in ESET products for Linux

2022-02-24 - Mitchell | ESET Nederland - Comments (0) - Customer Advisories

ESET Customer Advisory 2022-0005
February 24, 2022
Severity: Medium

Summary

ESET discovered a vulnerability in its business and server products for Linux. Fixed product versions are now available to download and ESET recommends that customers download and install them.

Details

As part of an internal code review process, ESET discovered a potential use-after-free vulnerability in a kernel module of its business and server products for Linux. This vulnerability could, in theory, allow an attacker to trigger a denial-of-service condition on the system.

ESET fixed the vulnerability and prepared new builds of its products that are now available to download.

The CVE ID reserved by ESET for this vulnerability is CVE-2022-0615 with the following CVSS v3 vector: AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C.

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

Solution

ESET prepared the following fixed product versions that are not susceptible to the vulnerability and recommends that users update to them:

- ESET Endpoint Antivirus for Linux version 7.1.10.0
- ESET Endpoint Antivirus for Linux version 8.1.7.0
- ESET Server Security for Linux version 7.2.578.0
- ESET Server Security for Linux version 8.1.818.0

Affected programs and versions

The following product versions are susceptible to the vulnerability:

- ESET Endpoint Antivirus for Linux from version 7.1.6.0 to 7.1.9.0
- ESET Endpoint Antivirus for Linux from version 8.0.3.0 to 8.1.5.0
- ESET Server Security for Linux from version 7.2.463.0 to 7.2.574.0
- ESET Server Security for Linux from version 8.0.375.0 to 8.1.813.0

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 discovered this vulnerability internally.

Version log

Version 1.0 (February 24, 2022): Initial version of this document