[CA8298] Vulnerability fixed in ESET Endpoint Encryption and ESET Full Disk Encryption for Windows

2022-08-01 - Mitchell | ESET Nederland - Comments (0) - Customer Advisories

ESET Customer Advisory 2022-0012
July 27, 2022
Severity: Medium

Summary

ESET became aware of a vulnerability in ESET Endpoint Encryption and ESET Full Disk Encryption for Windows that enables a user logged into the system to cause a blue screen error (BSOD).

Details

The vulnerability in the driver `dlpfde.sys` enables a user logged into the system to perform system calls leading to kernel stack overflow, resulting in a system crash, for instance, a BSOD.

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

The CVE ID reserved by ESET for this vulnerability is CVE-2022-2402 and the CVSS v3.1 base score is 6.5 with the following vector: `AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H`.

Solution

ESET has released fixed versions of ESET Endpoint Encryption and ESET Full Disk Encryption for Windows. We recommend users of the earlier, affected versions schedule upgrades to the fixed versions as soon as possible.

For ESET Full Disk Encryption for Windows, ESET recommends upgrading from the ESET PROTECT console.

For ESET Endpoint Encryption for Windows, a reinstallation is recommended. Users can upgrade client machines to a later version of ESET Endpoint Encryption.

The issue is resolved in the following builds:

- ESET Endpoint Encryption 5.1.2.26
- ESET Full Disk Encryption 1.3.2.32

Affected programs and versions

- ESET Endpoint Encryption 5.1.1.14 and earlier
- ESET Full Disk Encryption 1.3.1.25 and earlier

Feedback & support

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

Acknowledgment

ESET values the principles of coordinated disclosure within the security industry and would like to thank @SecAndStuff.

Version log

Version 1.0 (July 27, 2022): Initial version of this document