Release Notes

Entrust® LXM Card Printer Driver for Linux®, Version 1.9

This document provides a summary of updates to the LXM Card Printer Driver for Linux.

Version Information

Driver Version	1.9
Release Date	April 2026

Supported Printers

- Entrust® SD Series: SD260™, SD360™, SD460L™
- Entrust® CD Series: CD800™, CD820™ with Laminator Impresser
- Entrust® Artista® CR805, Artista® CR805 with Card Lamination Module, CE875 with Embosser/Indenter Module
- Entrust® Sigma DS1, DS2, DS3 with Card Lamination Module
- Entrust® Sigma DS3 with 600 DPI Module
- Entrust® Sigma DS4 Kiosk with Rear Indent Module, DS4 Kiosk with Embosser/Indenter Module

Other Entrust printers may be supported through the use of an RFID upgrade kit.

Supported Operating Systems and Platforms

The Linux 1.9 printer driver supports the following operating systems and platforms:

- Ubuntu 20.04, AMD64
- Ubuntu 24.04, AMD64
- Fedora 43, AMD64

> The Attribution table is no longer installed as part of the driver installation. It is available in the install package in the same location as the install and uninstall scripts. The filename is Entrust_Linux_Driver_OSS_Statement.html.

528187-001, Rev. H
April 2026

New Features

- Added specific resolution support for printers:
  - 300x600 DPI on Sigma.
  - 600x300 and 600x600 DPI on Sigma with 600 DPI support.
- You no longer need to have a USB printer connected and powered on to start the printer driver install. The installer will prompt you to power on and connect the printer when needed. Make sure you do not have both a USB and an Ethernet cable connected to a printer when installing the printer driver.
- There is a new application under the SDK samples to test printers with RIM. The following features are supported:
  - Magstripe encode
  - Magstripe read
  - Single-wire Duali
  - Print
  - Kiosk
  - Rear indent

  For more information, refer to the topic "RIMMagReadSmartCard Sample" in the *LXM Card Printer Driver for Linux® User's Guide*.
- Error messages are now displayed in the operating system locale language (previously it was always English):
  - Arabic
  - Brazilian Portuguese
  - Chinese Simplified
  - Chinese Traditional
  - Czech
  - English
  - French
  - German
  - Japanese
  - Korean
  - Polish
  - Romanian
  - Russian
  - Spanish

Improvements and Resolved Issues

- For the Ubuntu installer, driver artifacts are no longer installed in /usr/local/ and /usr/lib64/. Those paths are now /usr/share/ and /usr/lib/. This resolves warnings that were displayed after uninstall.

Known Issues and Restrictions

- Driver is supported only on a 64 bit AMD64 operating system.
- Renaming the printer requires a PC Reboot.
- After clicking the Test Page button on the Printer Options dialog box, no test page is printed but it is queued in Active Jobs. Entrust recommends using CUPS server, rather than the Printer Options dialog box, to print the test page. Refer to the topic "Printer Properties" in the *LXM Card Printer Driver for Linux® User's Guide*.
- When using Ubuntu 24.04, and when using the CUPS server Test Page, Impresser is not supported.
- UV ribbon is not supported.
- Escape codes are not supported (Laminator, Magnetic Stripe, Emboss, Indent, Topcoat Add, Topcoat Remove, Print Block, and Input Hopper).
- Rotation is not supported while using smartcard or magstripe on Artista Printers.
- Driver upgrade is not supported. Uninstall and reinstall to upgrade the driver.
- You must change Printer Options to select the printer type, ribbon type and page size to print properly.
- Printer status SDK does not return the correct ribbon supply part number.
- The Reverse Portrait and Reverse Landscape orientation options are not used by the printer driver. To achieve the same effect, set the "Rotate Card Image 180 Degrees" option in the printer settings for printer being printed to.
- The Linux driver supports only one USB printer connected to the same host.
- Multiple-copy printing is not supported.
- When the driver is set to Simplex and a multi-page job is sent, all pages other than page 1 are discarded.

Not Supported for Version 1.9

- Kylin operating system.

Vulnerabilities

CVE-2026-31431

CVE-2026-31431 is an escalation of privilege exploit that works on any unpatched Linux distribution with a kernel version from 4.14 to 6.19.12. This exploit is with the Linux kernel and not with the Entrust LXM Card Printer Driver. The driver does not increase the attack surface for this exploit. However, someone exploiting this vulnerability could potentially intercept or manipulate printer driver requests.

For more information:

- Overview of the exploit from the team that found it: https://copy.fail/

- The CVE record: https://www.cve.org/CVERecord?id=CVE-2026-31431

Ubuntu Users:

Ubuntu page describing how to patch Ubuntu: https://ubuntu.com/blog/copy-fail-vulnerability-fixes-available

Fedora Users:

Manually check the kernel version. This can be done via: "uname -r".

This gives an output like "6.19.13-200.fc43.x86_64".

The patched kernel versions are 6.18.22+, 6.19.12+, and 7.0+. Any version older than those should be patched.

To patch this, a full system upgrade can be done via: "sudo dnf upgrade".

To only update the kernel: "sudo dnf upgrade 'kernel*'" (note the single quotes)

CVE-2026-43284 and CVE-2026-43500

CVE-2026-43284 affects Linux kernel versions from January 1, 2017 up to May 5, 2026.

CVE-2026-43500 affects Linux kernel versions from June 8, 2023 up to May 10, 2026.

While no patched kernels have been released yet, there are steps to mitigate the issue.

It is an escalation of privilege exploit. This exploit is with the Linux kernel and not with the Entrust LXM Card Printer Driver. The driver does not increase the attack surface for this exploit. However, someone exploiting this vulnerability could potentially intercept or manipulate printer driver requests.

For more information:

- Overview of the exploit from the team that found it: https://github.com/V4bel/dirtyfrag
- The CVE records:
  - https://www.cve.org/CVERecord?id=CVE-2026-43284
  - https://www.cve.org/CVERecord?id=CVE-2026-43500

Ubuntu Users:

https://ubuntu.com/blog/dirty-frag-linux-vulnerability-fixes-available

Fedora Users:

Fedora users should run the step under the "Mititgation" section in the GitHub link (V4bel/dirtyfrag (github)).