

Entrust Security Bulletin E24-004

Possible case of Local Privilege Escalation (LPE) vulnerability (CVE-2024-34329)

May 31, 2024

Who should read this bulletin

Customers using the Datacard XPS Card Printer Driver Version 8.5 or earlier.

Summary

A possible local privilege escalation vulnerability was found affecting the Datacard XPS Card Printer Driver. A user with unprivileged access to a system on which the driver is installed could gain administrative privileges on that system.

Users of Datacard XPS Card Printer Driver Version 8.5 or earlier are urged to implement the changes described in the Corrective Action section below.

Impact of Vulnerability

Due to insecure file/folder permissions applied to the Datacard XPS Card Printer Driver files during installation, an attacker having unprivileged access to a system with the driver installed could gain administrative privileges. This issue affects Datacard XPS Card Printer Driver Version 8.5 and earlier.

Mitigating Factors

- There are no known cases involving the exploitation of this vulnerability among Entrust's customers.
- An attacker exploiting this vulnerability would need access to the system where Card Printer Driver is installed.

Corrective Action

A patch (part number 528504-001) has been created for the Datacard XPS Card Printer Driver Versions 8.4 and 8.5 which corrects the permissions on the affected files. Customers having installed the driver are strongly recommended to install this patch.

Customers using an older version of the driver should upgrade to version 8.5 and apply the patch.

Support

Entrust Support can be contacted using our standard methods:

- Email: support@entrust.com
- Support Portal: <https://trustedcare.entrust.com/login>
- Phone: [support numbers](#)

To setup a new Trusted Care account, where you can view and receive future security bulletins, please email: trustedcare@entrust.com.

© Copyright 2024 Entrust Corporation. All rights reserved.

Entrust is a trademark or a registered trademark of Entrust, Inc. in the United States and certain countries. All Entrust product names and logos are trademarks or registered trademarks of Entrust, Inc. or Entrust Corporation. All other company and product names and logos are trademarks or registered trademarks of their respective owners in certain countries.

Given the very nature of security vulnerabilities, security bulletins are intended to be kept to a small group of individuals. Security bulletins are to be distributed within your company only, and only on a need to know basis.

The information in this bulletin is proprietary and confidential to Entrust Corporation, and its subsidiaries, and any disclosure of this information is governed by the confidentiality terms in the agreement pursuant to which you obtained a license for the referred to Entrust products.

The information in this bulletin is provided "as is" by Entrust without any representations, conditions and/or warranties of any kind, whether express, implied, statutory, by usage of trade, or otherwise. Entrust specifically disclaims any and all representations, conditions, and/or warranties of merchantability, satisfactory quality, and/or fitness for a particular purpose. To the maximum extent permitted by applicable law, in no event will Entrust be liable for any damages, losses or costs arising from your or any third party actions or omissions in connection with this bulletin. The only representations, conditions and/or warranties that may be applicable to any Entrust products that you may have are those contained in the agreement pursuant to which you obtained a license for those Entrust products.