

Entrust Security Bulletin E25-002

Unauthenticated arbitrary file reading and arbitrary code execution vulnerability in Printer Manager systems

Who should read this bulletin

Customers with printers running D3.18.4-3 or prior firmware with Printer Manager enabled (the default configuration). Customers with this configuration are advised to upgrade to the latest version and apply the remediation steps described herein.

Summary

An unauthenticated arbitrary file reading and arbitrary code execution vulnerability has been identified in printers with the Printer Manager component. Users of affected versions of Printer Manager are urged to implement the changes described in the Corrective Action section below.

Impact of Vulnerability

The unauthenticated arbitrary file reading and arbitrary code execution vulnerability exists in printers that have the Printer Manager component enabled. This vulnerability could allow an attacker with network access to the Printer Manager interface to read arbitrary files housed on the printer or to execute arbitrary code on the printer.

Mitigating Factors

- Exploiting this vulnerability is not possible when the Printer Manager port has been disabled. Disabling the Printer Manager port is an existing recommended best practice.
- There are no known cases involving the exploitation of this vulnerability among Entrust's customers.

Corrective Action

Entrust recommends that the affected printers be updated to D3.20.1 firmware, which is available on the [Entrust CD800 Series ID Card Printer Support web page](#). This will resolve the vulnerability as well as bring forward the printer's operating system and patches to 2025 levels.

It is also recommended as a security best practice that the Printer Manager port be disabled during card production to minimize the attack surface. The Printer Manager can be re-enabled when printer servicing is required.

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 2025 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.