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.