

Entrust Security Bulletin E25-003a

Vulnerabilities in Instant Financial Issuance On Premise Software

March 12, 2025

Who should read this bulletin

Customers of Instant Financial Issuance (IFI) On Premise software are affected as outlined below:

- IFI On Premise 6.10.x up to 6.10.2, inclusive
- IFI On Premise 6.9.x up to 6.9.3, inclusive
- IFI On Premise 6.8.x and older

Customers using the above versions of IFI On Premise software are advised to apply the remediation steps and upgrade to the latest version described herein.

Summary

Vulnerabilities have been identified in Instant Financial Issuance (IFI) On Premise software that could allow remote code injection, arbitrary file write, and arbitrary file read under certain conditions.

Customers of affected versions of IFI On Premise software are urged to implement the changes described in the Corrective Action section below.

Impact of Vulnerability

For the IFI On Premise software, an attacker having administrative privileges and in-depth knowledge of how to use Output File Templates with Template Manager could execute remote code, and read and write arbitrary files on the server.

The vulnerability cannot be exploited when the Output File Templates with Template Manager feature is not enabled. However, it is important to note that an attacker with IFI On Premise administrator credentials could enable this feature and then exploit the vulnerability.

Mitigating Factors

- There are no known cases involving the exploitation of this vulnerability among Entrust's customers.
- Successful exploitation of any of these vulnerabilities requires administrative privileges as well as detailed product knowledge.

Corrective Action

Customers of affected versions of IFI On Premise software are strongly recommended to review **Template Manager Recommendations** available on Trusted Care to assist with determining whether you use Template Manager and how best to harden usage (before and after applying the patch) and deploy an available patch/release as outlined in this table:

Impacted Version	Recommended Release/Patch
IFI On Premise 6.10.x up to 6.10.2	IFI On Premise 6.10.3
IFI On Premise 6.9.x up to 6.9.3	IFI On Premise 6.9.4
IFI On Premise 6.8.x and older	Already reached End of Life. Recommend to upgrade to the latest fully patched version (i.e. 6.10.3 at the time of this bulletin)

Support

Entrust Support can be contacted using our standard methods:

- Email: CustomerCare@entrust.com
- Phone: [support numbers](#)

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