Entrust Security Bulletin E25-005a

Arbitrary File Write vulnerability in Instant Financial Issuance as a Service (IFIaaS) Software

March 12, 2025

Who should read this bulletin

Customers of Instant Financial Issuance as a Service (IFIaaS) software are affected as outlined below:

- IFIaaS tenant components 8.1.2, 8.2.0 and 8.2.1

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

Summary

Arbitrary File Write vulnerability has been identified in Instant Financial Issuance as a Service (IFIaaS) software.

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

Impact of Vulnerability

Due to this vulnerability, an attacker having administrative privileges and in-depth knowledge of how to use Output File Templates with Template Manager could write arbitrary files only within the IFI Tenant components, but not within the IFIaaS server components.

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 IFIaaS 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 this vulnerability requires administrative privileges as well as detailed product knowledge.

Corrective Action

Customers of affected versions of IFIaaS software are strongly recommended to review **Template Manager Recommendations** available on Trusted Care to assist with determining whether they 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
IFIaaS tenant components 8.1.2, 8.2.0 and 8.2.1	Recommend to upgrade the tenant components to 8.2.5 or higher

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.

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.