Saviynt Enterprise Identity Cloud vulnerable to local user enumeration and authentication bypass

Vulnerability Note VU#692873

Original Release Date: 2021-12-22 | Last Revised: 2022-02-02

ABOUT VULNERABILITY NOTES

CONTACT US ABOUT THIS VULNERABILITY

PROVIDE A VENDOR STATEMENT

Overview

Saviynt Enterprise Identity Cloud contains user enumeration and authentication bypass vulnerabilities in the local password reset feature. Together, these vulnerabilities could allow a remote, unauthenticated attacker to gain administrative privileges if an SSO solution is not configured for authentication.

Description

Saviynt Enterprise Identity Cloud contains two vulnerabilities in the password reset feature for the local authentication system. Specifying the `id` parameter returns user names and it is common that accounts with administrative privileges have low (often single digit) `id` values.

```
/ECM/maintenance/forgotpasswordstep1?otpConfig=false&id=5
```

It is then possible to either unhide a button or directly access a URL that bypasses verification and allows the password to be changed. Accessing a login URL with the new credentials yields cookies that can be used to authenticate to the Enerprise Identity Cloud instance.

If another authentication or SSO system is configured, then it is not possible to exploit these vulnerabilities.

Impact

A remote, unauthenticated attacker can enumerate users and bypass authentication to change the password of an existing administrative user. The attacker can then perform administrative actions and possibly make changes to other connected authentication systems.

Solution

Saviynt has deployed a backend update for the software that resolves the issue in Saviynt IGA Release v5.5 SP2.x and later versions. As an additional layer of security, as the impacted URLs are not commonly used by customers leveraging SSO, Saviynt has blocked access to the URLs needed to exploit these vulnerabilities.

Saviynt users should not need to take any action but might want to confirm they are running a fixed version.

Acknowledgements

This document was written by Eric Hatleback and Art Manion.

Vendor Information

Filter by status:

All

Filter by content:

□ Additional information available

Sort by:

Status

Expand all

Saviynt Affected

Other Information

Date Public:	2021-12-22
Date First Published:	2021-12-22
Date Last Updated:	2022-02-02 20:11 UTC
Document Revision:	5

Sponsored by CISA.

Download PGP Key

Read CERT/CC Blog

Learn about Vulnerability Analysis

Carnegie Mellon University
Software Engineering
Institute
4500 Fifth Avenue
Pittsburgh, PA 15213-2612
412-268-5800

Contact SEI

Contact CERT/CC

☎ 412-268-5800
✉ cert@cert.org

Office Locations | Additional Sites Directory | Legal | Privacy Notice |
CMU Ethics Hotline | www.sei.cmu.edu