



Security Incident Report

Date: October 24, 2019

Type: Escalation of Privileges

Description

EnergyCAP staff was made aware by a customer of peculiar behavior with publicly shared dashboards on October 11, 2019. On October 23, 2019, EnergyCAP Technology staff were able to recreate the issue and verify that the vulnerability did exist. In certain scenarios, a user could impersonate the creator of a public dashboard by following a link within the dashboard.

Remediation

As a temporary remediation, EnergyCAP Technology disabled access to any public dashboards via firewall rule. In the meantime, a fix for the vulnerability was developed and tested. A new build (v7.5.7) was reviewed, tested, and released according to Change Advisory Board processes. EnergyCAP Technology also implemented additional measures to further restrict the ability of public dashboard users to call other APIs not associated with dashboard content. This update was also merged into the latest release (v7.5.7).

EnergyCAP clients that host their own instance of EnergyCAP Version 7 are being notified, and a build of EnergyCAP Version 7.5.7 will be made available to them. As an interim fix, a database script that will disable any previously created public dashboards will be available to download from the [EnergyCAP Support](#) website.

Impacted Services

- EnergyCAP Version 7 Public Dashboards

Impacted Data

The vulnerability could allow a malicious dashboard user to elevate privileges and access EnergyCAP services with the rights of the EnergyCAP user who created the public dashboard. As such, all data and rights associated with the EnergyCAP user were potentially vulnerable.

Disclosure Timeline

ALL TIMES IN EST

2019-10-11 7:37am	EnergyCAP staff made aware of unexpected results with configuring public dashboards
2019-10-23 2:30pm	Vulnerability recreated and verified
2019-10-23 5:53pm	Software fix developed
2019-10-23 7:18pm	Feature blocked for hosted clients
2019-10-24 12:00am	Company notified
2019-10-24 11:00am	Software fix testing completed
2019-10-24 12:52pm	Build released to production environment
2019-10-24 9:00pm	Public Disclosure
2019-10-24 11:00pm	Planned updated release of v7.5.7 with additional API restrictions for public dashboard users
2019-10-25 9:00pm	Final release of v7.5.7 expected to be available to self-hosted clients

Contact

Please direct information security questions to:

Adam Hegedus

Chief Security Officer

EnergyCAP, Inc.

Email: adam.hegedus@energycap.com