Weak policy at Change password function in kromitgmbh/titra

0

Valid Reported on Jun 12th 2022

Description

We can register an normal account with >= 8 characters password. But we ccan change password with just 1 character when we use change password function

Proof of Concept

https://drive.google.com/file/d/1D-IDqrMiaBGLnZaZY9L3u-S4u-MoGxPc/view?usp=

Impact

When users change password to a too simple password, attacker can easily guess user password and access account.

CVE
CVE-2022-2098
(Published)

Vulnerability Type
CWE-521: Weak Password Requirements

Severity
High (7.1)

Registry
Other

Affected Version
<=0.78.0

Visibility

Public

Status
Fixed

Found by

Tran Duc Anh
@kmaron1n
master

This report was seen 547 times.

We are processing your report and will contact the **kromitgmbh/titra** team within 24 hours.
5 months ago

We have contacted a member of the **kromitgmbh/titra** team and are waiting to hear back
5 months ago

A **kromitgmbh/titra** maintainer validated this vulnerability 5 months ago

Tran Duc Anh has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Tran Duc Anh 5 months ago — Researcher

@admin can we assign a CVE to this vulnerability?

Jamie Slome 5 months ago — Admin

If the maintainer is happy to proceed with a CVE, we will assign and publish one on their behalf.

@maintainer?

A **kromitgmbh/titra** maintainer marked this as fixed in **0.78.1** with commit

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

A **kromitgmbh/titra** maintainer 5 months ago

I am okay with a CVE but the vulnerability has just been fixed in the latest version of titra (0.78.1).

Jamie Slome 5 months ago Admin

Sorted 👍

@maintainer - it is good and standard practice to publish CVEs, especially after they have been fixed :)

Sign in to join this conversation