nextauthjs / **next-auth** Public

Code | Issues 98 | Pull requests 74 | Discussions | Actions | Projects | ···

Insecure email token verification in Prisma adapter

Critical **iaincollins** published **GHSA-pg53-56cg-4m8q** on Feb 10, 2021

Package

next-auth (npm)

Affected versions	Patched versions
< 3.3.0	3.3.0

Description

Impact

Implementations using the **Prisma database adapter** with the **Email provider are impacted**.

Implementations using the Prisma database adapter that are not using the Email provider are not impacted.
Implementations using the default database adapter (TypeORM) with the Email provider are not impacted.
Implementations not using a database are not impacted.

Patches

This issue is fixed in 3.3.0 and newer versions.

Workarounds

Those not able to upgrade can alternatively disable the Email provider as a workaround.

Description

The Prisma database adapter was checking the verification token but not the identifier (the email address associated with the token). This made it possible to use a valid token assigned to one user, to sign in as another user when using the Prima adapter in conjunction with the Email provider. The defect is specific to the community-supported Prisma database adapter in versions <3.3.0 and is not present in the default database adapter (TypeORM).

Note: The current community-supported adapter was not developed by Prisma.

The defect was a problem in the implementation of verification function the adapter and is not directly related to Prisma.

The flaw may exist in other third party database adapters that do not check both the identifier and token values.

The design of the database adapter API may be revised in future to help reduce the likelyhood of similar defects.

Timeline

On Monday (2021-02-08) we were notified via responsible disclosure by Alessandro Angelino (**@AlessandroA**) of a flaw in the implementation of the Prisma database adapter included with NextAuth.js. A detailed write up and proof of concept were provided.

The following day (2021-02-09) we published a fix in v3.3.0 and confirmed through internal testing, and with Alessandro, that the issue was resolved in the new release and prompted users to upgrade.

On 2021-02-10 we received a CVE ID and published this advisory within a few hours of notification.

We would like to thank Alessandro for using responsible disclose to allow us to address the issue promptly and publish this advisory once an update was available that resolved the issue and Balázs Orbán (**@balazsorban44**) for facilitating a timely release of the fix.

Severity

Critical

CVE ID

CVE-2021-21310

Weaknesses

No CWEs

Credits

AlessandroA
balazsorban44
iaincollins