

Field-level access-control bypass for multiselect field

Critical dcousens published GHSA-6mhr-52mv-6v6f on Oct 17

Package

 @keystone-6/core (npm)

Affected versions

2.2.0 || 2.3.0

Patched versions

2.3.1

Description

Impact

@keystone-6/core@2.2.0 || 2.3.0 users who are using the `multiselect` field, and provided field-level access control - are vulnerable to their field-level access control not being used.

List-level access control is **NOT** affected.

Field-level access control for fields other than `multiselect` are **NOT** affected.

Example, **you are vulnerable** if you are using field-level access control on a `multiselect` like the following:

```
const yourList = list({
  access: {
    // this is list-level access control, this is NOT impacted
  },
  fields: {
    yourFieldName: multiselect({
      // this is field-level access control, for multiselect fields
      // this is vulnerable
      access: {
        create: ({ session }) => session?.data.isAdmin,
        update: ({ session }) => session?.data.isAdmin,
      },
      options: [
        { value: 'apples', label: 'Apples' },
        { value: 'oranges', label: 'Oranges' },
      ],
    })
  }
})
```

```
    ],  
    // ...  
  }},  
  // ...  
},  
// ...  
});
```

Mitigation

Please upgrade to `@keystone-6/core >= 2.3.1`, where this vulnerability has been closed.

Workarounds

If for some reason you cannot upgrade your dependencies, you should stop using the `multiselect` field.

Credits

Thanks to [Marek R](#) for reporting and submitting the pull request to fix this problem.

If you have any questions around this security advisory, please don't hesitate to contact us at security@keystonejs.com, or [open an issue on GitHub](#).

If you have a security flaw to report for any software in this repository, please see our [SECURITY policy](#).

Severity

Critical 9.1 / 10

CVSS base metrics

<u>Attack vector</u>	Network
<u>Attack complexity</u>	Low
<u>Privileges required</u>	None
<u>User interaction</u>	None
<u>Scope</u>	Unchanged
<u>Confidentiality</u>	High
<u>Integrity</u>	High
<u>Availability</u>	None

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N


CVE ID

CVE-2022-39322

Weaknesses

No CWEs

Credits

 **marekryb**