

Weak Password Requirements in notrinos/notrinoserp

0



Reported on Aug 18th 2022

Description

The product does not require that users should have strong passwords, which makes it easier for attackers to compromise user accounts.

Proof of Concept

Steps to reproduce

1. Login to admin account.
2. From user account setup create a new user.
3. Fill the form username `user3` and password single character `a`.
4. Account created successfully without any password restriction.

The screenshot displays the 'Users' management page in the NotrinosERP application. The page shows a table of existing users and a form to add a new user. The form fields are filled with the following data:

User login	Full Name	Phone	E-mail	Last Visit	Access Level
admin	Administrator		adm@example.com	08/18/2022 04:21 pm	System Administrator
user1	user1			08/18/2022 04:20 pm	AP Officer
user2	user2			08/18/2022 03:16 pm	Inquiries

The 'Add new user' form is shown below the table. The 'User Login' field is set to 'user3'. The 'Password' field is highlighted with a red box and a red circle, indicating it is the focus of the attack. The 'Full Name' field is empty. The 'Telephone No.' field is empty. The 'Email Address' field is empty. The 'Access Level' dropdown is set to 'AP Officer'. The 'Language' dropdown is set to 'English'. The 'User's POS' dropdown is set to 'Default'. The 'Printing profile' dropdown is set to 'Browser printing support'. The 'Use popup window for reports' checkbox is checked. The 'Add new' button is highlighted with a red box and a red circle, indicating it is the next step in the process.

Below the form, a green message bar states: 'A new user has been added.'

The footer of the page shows the date and time: '08/18/2022 | 04:27 pm' and the version: 'NotrinosERP 0.7 - Theme: default'.

Chat with us

user1	user1		08/18/2022 04:20 pm	AP Officer		
user2	user2		08/18/2022 03:16 pm	Inquiries		
user3			01:00 am	AP Officer		

☐ Show also inactive

Impact

An attacker could easily guess user passwords and gain access user accounts.

References

- [CWE](#)

CVE

CVE-2022-2927

(Published)

Vulnerability Type

CWE-521: Weak Password Requirements

Severity

High (7.3)

Registry

Other

Affected Version

<=0.7

Visibility

Public

Status

Fixed

Found by



Abdullah Baghuth

@0xcybery

amateur 

Fixed by



Phương

@notrinos

unranked 

Chat with us

This report was seen 618 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

♥ **Phường** gave praise 3 months ago

Thanks @0xcybery for detecting this, will fix it soon

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

Phường assigned a CVE to this report 3 months ago

Phường validated this vulnerability 3 months ago

Abdullah Baghuth has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Phường marked this as fixed in 0.7 with commit **e61e76** 3 months ago

Phường has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Sign in to join this conversation

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us