huntr

Account Takeover in neorazorx/facturascripts

0

✓ Valid Reported on May 9th 2022

Description

Hi there i found that forget password functionality can be manipulated and this lead to account takeover. So even if an attacker can takeover low access user to admin accounts. In this bug server is vulnerable to php type juggling attack

Proof of Concept

While registering app for first use set DB password starting with "0e" and then random characters in it. so You can add any password starting with 0e
Goto forget password section and add username as admin and new password as "newpass"
Add 0 in database password
Send request and login with new password
Successfully changed password
Reference :-https://medium.com/swlh/php-type-juggling-vulnerabilities-3e28c4ed5c09

Impact

Account takeover

CVE
CVE-2022-1715
(Published)

Vulnerability Type
CWE-1125: Excessive Attack Surface

Severity
Critical (9.8)

Registry
Other

Affected Version

2022.06

Visibility

Public

Status

Fixed

Found by

Distorted_Hacker

@gaurav-g2

pro

Fixed by

Distorted_Hacker

@gaurav-g2

pro

This report was seen 622 times.

We are processing your report and will contact the **neorazorx/facturascripts** team within 24 hours. 7 months ago

Distorted_Hacker modified the report 7 months ago

Distorted_Hacker modified the report 7 months ago

Distorted_Hacker modified the report 7 months ago

Distorted_Hacker submitted a **patch** 7 months ago

Distorted_Hacker modified the report 7 months ago

We have contacted a member of the **neorazorx/facturascripts** team and are waiting to hear back 7 months ago

Distorted_Hacker submitted a **patch** 7 months ago

Carlos Garcia validated this vulnerability 6 months ago

Chat with us

Distorted_Hacker has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Carlos Garcia marked this as fixed in **2022.07** with commit **714beb** 6 months ago

Distorted_Hacker has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Distorted_Hacker 6 months ago Researcher

@admin can you please assign a CVE

Jamie Slome 6 months ago Admin

Sorted 👍

Sign in to join this conversation

huntr

home

hacktivity

leaderboard

part of 418sec

company

about

team

Chat with us

FAQ

contact us

terms

privacy policy

Chat with us