

27

Week Passwords generated by password reset function

Share:

State ○ Resolved (Closed)Disclosed **May 9, 2020 7:24pm +0530**Reported To **MTN Group**Asset
Mtn.co.za
(Domain)

Weakness Weak Password Recovery Mechanism for Forgotten Password

Severity ○ Low (0.1 ~ 3.9)

Participants

Visibility Disclosed (Full)

[Collapse](#)

TIMELINE · EXPORT

tp9222 submitted a report to **MTN Group**.

Dec 27th (5 months ago)

Summary:

Assessor observed that password reset function generates only alphanumeric passwords that is passwords don't contain any special characters
Also User can set old password as new password.

Steps To Reproduce:Goto <https://mycontract.mtn.co.za/landing/landing.htm>

Click forget password link

select email radio button and enter user ID

press submit

Application will send email with week password

upon entering temporary password application ask user to set new password

here user can enter his immediate used password

Supporting Material/References:https://www.owasp.org/index.php/Authentication_Cheat_Sheethttps://www.owasp.org/index.php/Top_10-2017_A3-Sensitive_Data_Exposure**Remediation:**

Application should generate secure passwords that password should contain alphanumeric characters as well as special characters

Application should not allow user to set previously used 5 password as new password

Impact**Impact**

Brute force attack can be carried out on the password based authentication mechanism

1 attachment:

F669582: [password_reset_not_secure.jpg](#)cybersecurity_7ibu8 changed the status to ○ **Triaged**.

Jan 2nd (5 months ago)

sent for investigation



tp9222 posted a comment.

Mar 30th (2 months ago)

Hello, @cybersecurity_7ibu8 is vulnerability fixed?


vancora closed the report and changed the status to ○ **Resolved**.

Apr 9th (2 months ago)



tp9222 requested to disclose this report.

Apr 9th (2 months ago)

 This report has been disclosed.

May 9th (22 days ago)