

Report Details

Company	Acme
Domain Analysed	acme.com
Analysis Date and Time	2022/05/17 3:06:59 PM

Introduction

The following report is compiled from the metrics retrieved by running the Authlogics Password Audit Tool on your domain controllers to analyse the passwords currently in use in your organisation. Below are the findings highlighting the critical and high-risk areas we recommend addressing. Detailed information has been supplied as part of the audit.

Executive Summary

	Count	%	Risk
Accounts audited	5827		
Active accounts	3492	59.93	
Active accounts with breached passwords	787	13.51	High
Administrators with breached passwords	2	0.03	Critical
Accounts with breached passwords	1582	27.15	High
Accounts with commonly breached passwords	564	9.68	Critical
Breached accounts with identifiable information	30	0.51	Medium
Breached accounts with matching passwords	0	0	None
Accounts with shared passwords	2437	41.82	High
Emails for this domain with breached passwords	142	2.44	Medium

An audit was conducted, and out of the 5827 accounts, 1582 accounts (27.15%) have passwords that have been found in breaches. Of this number, 787 of the accounts (13.51%) are active and 2 (0.03%) belong to your administrators.

The fact that some administrator accounts have been found to have breached passwords is of great concern and requires immediate addressing.

The high number of shared passwords within the organisation is a concern and should be addressed.

The high percentage of accounts using breached passwords is of great concern and requires immediate addressing.

The high number of accounts using commonly breached passwords is of serious concern as these passwords are typically very weak and are easily guessed or brute-forced.

We detected [a number of](#) email accounts for this domain with breached passwords making these accounts subject to attack.