# AZURE SECURITY FIX - MASTER EXECUTION GUIDE

CRITICAL: Follow this guide step by step to fix 434 Azure security issues safely

## EXECUTIVE SUMMARY

Issues Found: 434 total

- Critical: 9

- High: 72

- Medium: 351

- Low: 2

Estimated Fix Time: 3-5 days

Production Impact: Minimal if following this guide

Rollback Plan: Included for each phase

## EXECUTION ORDER

Phase 1: Storage and Key Vault (Day 1) - ZERO RISK

Phase 2: Resource Governance (Day 1) - ZERO RISK

Phase 3: Network Security (Day 2-3) - MEDIUM RISK

Phase 4: RBAC and Permissions (Day 4) - HIGH RISK

Phase 5: Subscription Locks (Day 5) - LOW RISK

Phase 6: Verification (Day 5) - ZERO RISK

## PREREQUISITES

az login

az account set --subscription "YOUR\_SUBSCRIPTION\_ID"

New-Item -ItemType Directory -Path "C:\Azure-Fixes-Backup" -Force

az account show > C:\Azure-Fixes-Backup\subscription-info.json

az role assignment list --all > C:\Azure-Fixes-Backup\rbac-before.json

az network nsg list > C:\Azure-Fixes-Backup\nsg-before.json

## PHASE 1: STORAGE ACCOUNT FIXES

Risk: LOW

Time: 30 minutes

Issues Fixed: 100-150

$storageAccounts = az storage account list --query "[].{name:name, resourceGroup:resourceGroup}" -o json | ConvertFrom-Json

foreach ($sa in $storageAccounts) {

az storage account update --name $sa.name --resource-group $sa.resourceGroup --https-only true

az storage account update --name $sa.name --resource-group $sa.resourceGroup --min-tls-version TLS1\_2

az storage account update --name $sa.name --resource-group $sa.resourceGroup --allow-blob-public-access false

}

## PHASE 2: KEY VAULT FIXES

Risk: LOW

Time: 15 minutes

$keyVaults = az keyvault list --query "[].{name:name}" -o json | ConvertFrom-Json

foreach ($kv in $keyVaults) {

az keyvault update --name $kv.name --enable-soft-delete true

az keyvault update --name $kv.name --enable-purge-protection true

}

## PHASE 3: NETWORK SECURITY

Risk: MEDIUM

Time: 2-4 hours

$nsgs = az network nsg list -o json | ConvertFrom-Json

$dangerousRules = @()

foreach ($nsg in $nsgs) {

$rules = az network nsg rule list --nsg-name $nsg.name --resource-group $nsg.resourceGroup -o json | ConvertFrom-Json

foreach ($rule in $rules) {

if ($rule.direction -eq "Inbound" -and $rule.access -eq "Allow" -and $rule.sourceAddressPrefix -eq "\*") {

$dangerousRules += [PSCustomObject]@{

NSG = $nsg.name

ResourceGroup = $nsg.resourceGroup

RuleName = $rule.name

Port = $rule.destinationPortRange

}

}

}

}

$dangerousRules | Export-Csv "C:\Azure-Fixes-Backup\dangerous-nsg-rules.csv" -NoTypeInformation

## PHASE 4: RBAC AND PERMISSIONS

Risk: HIGH - Get approval first

$allRoles = az role assignment list --all -o json | ConvertFrom-Json

$staleAssignments = $allRoles | Where-Object { [string]::IsNullOrEmpty($\_.principalName) }

foreach ($assignment in $staleAssignments) {

az role assignment delete --ids $assignment.id

}

## PHASE 5: SUBSCRIPTION LOCKS

az lock create --name "PreventAccidentalDeletion" --lock-type CanNotDelete --resource-group "YOUR\_CRITICAL\_RG"

## PHASE 6: VERIFICATION

cd "D:\PYEX-AVD-Deployment"

.\Analyze-AzureEnvironment.ps1

## ROLLBACK

Network: az network nsg rule update --resource-group RG --nsg-name NSG --name RULE --source-address-prefixes "\*"

RBAC: az role assignment create --assignee USER --role "Owner" --scope "/subscriptions/SUB\_ID"

Last Updated: 2025-10-13