Check ID	File	Resource	Check Name	Line	Possible CVE/CWE	Guideline URL	Status
CKV_AZURE_160	/main.tf	azurerm_network_security_group.sg-automate-test	Ensure that HTTP (port 80) access is restricted from the internet	37-86	1. CVE-2017-5689: Improper Access Restriction 2. CWE-211: Information Leak Through Query Strings in GET Request 3. CWE-79: Improper Neutralization of Input During Web Page Generaton (Cross-site Scripting)	https://docs.bridgecrew.io/docs/ensure-azure-http-port-80-access-from-the-internet-is-restricted	FAILED
CKV_AZURE_10	/main.tf	azurerm_network_security_group.sg-automate-test	Ensure that SSH access is restricted from the internet	37-86	1. CVE-2018-15473: Improper Access Restrictions 2. CWE-287: Improper Authentication 3. CWE-264: Permissions Privileges and Access Controls	https://docs.bridgecrew.io/docs/bc_azr_networking_3	FAILED
CKV_AZURE_50	/main.tf	azurerm_linux_virtual_machine.vmachine-automate-test	Ensure Virtual Machine Extensions are not Installed	127-167	1. CVE-2020-1530: RCE Weak Authentication on Linux VM 2. CWE-77: Improper Neutralization of Special Elements. 3. CVE-2020-0190: Unsecured Azure VM Connections.	https://docs.bridgecrew.io/docs/bc_azr_general_14	FAILED
CKV_AZURE_179	/main.tf	azurerm_linux_virtual_machine.vmachine-automate-test	Ensure VM agent is installed	127-167			FAILED
CKV_AZURE_119	/main.tf	azurerm_network_interface.nic-automate-test	Ensure that Network Interfaces don't use public IPs	113-124	of each 1. CVE-2018-1400: Cross Site Request Forgery allowing attackers to submit unauthenticated requests and inject malicious code. 2. CVE-2019-8792: Improper Input Validation which can lead to unintended data manipulation and lack of data protection. 3. CVE-2020-6888: Resource Exhaustion which can allow malicious actors to exhaust system memory or otherwise cause the system to consume resources excessively.	https://docs.bridgecrew.io/docs/ensure-that-network-interfaces-dont-use-public-ips	FAILED
CKV_AZURE_183	/main.tf	azurerm_virtual_network.vn-automate-test	Ensure that VNET uses local DNS addresses	16-26			PASSED
CKV_AZURE_182	/main.tf	azurerm_virtual_network.vn-automate-test	Ensure that VNET has at least 2 connected DNS Endpoints	16-26			PASSED
CKV_AZURE_9	/main.tf	azurerm_network_security_group.sg-automate-test	Ensure that RDP access is restricted from the internet	37-86		https://docs.bridgecrew.io/docs/bc_azr_networking_2	PASSED
CKV_AZURE_77	/main.tf	azurerm_network_security_group.sg-automate-test	Ensure that UDP Services are restricted from the Internet	37-86		https://docs.bridgecrew.io/docs/ensure-that-udp-services-are-restricted-from-the-internet	PASSED
CKV_AZURE_118	/main.tf	azurerm_network_interface.nic-automate-test	Ensure that Network Interfaces disable IP forwarding	113-124		https://docs.bridgecrew.io/docs/ensure-that-network-interfaces-disable-ip-forwarding	PASSED
CKV_AZURE_1	/main.tf	azurerm_linux_virtual_machine.vmachine-automate-test	Ensure Azure Instance does not use basic authentication(Use SSH Key Instead)	127-167		https://docs.bridgecrew.io/docs/bc_azr_networking_1	PASSED
CKV_AZURE_178	/main.tf	azurerm_linux_virtual_machine.vmachine-automate-test	Ensure linux VM enables SSH with keys for secure communication	127-167			PASSED
CKV_AZURE_149	/main.tf	azurerm_linux_virtual_machine.vmachine-automate-test	Ensure that Virtual machine does not enable password authentication	127-167		https://docs.bridgecrew.io/docs/ensure-azure-virtual-machine-does-not-enable-password-authentication	PASSED
CKV_AZURE_92	/main.tf	azurerm_linux_virtual_machine.vmachine-automate-test	Ensure that Virtual Machines use managed disks	127-167		https://docs.bridgecrew.io/docs/ensure-that-virtual-machines-use-managed-disks	PASSED