CHG0030003 — [TITAN] Critical — security on nsg-titan-webtier

Severity	Critical	Priority	1 - Critical
Cloud	Azure	State	New
Resource	nsg-titan-webtier	Group	network_operations
Resource type	Microsoft.Network/networkSecurityGroups	Change type	Normal
Opened	2026-04-21 14:36:43	Closed	2026-04-21 14:36:43
CAB required	Yes	Close code	—

Security Finding

```
NSG rule AllowSSHAll permits SSH (port 22) from 0.0.0.0/0 — Internet-wide privilege escalation
path to every VM in the subnet.
```

Justification

```
NSG rule AllowSSHAll permits SSH (port 22) from 0.0.0.0/0 — Internet-wide privilege escalation
path to every VM in the subnet.
```

Implementation Plan

```
1. Pre-change snapshot captured by TITAN (auto-rollback available).
2. Execute fix command:
az network nsg rule update --name AllowSSHAll --nsg-name nsg-titan-webtier --resource-group
rg-titan-demo --source-address-prefixes VirtualNetwork
3. TITAN FORGE verifies the fix was applied.
4. Post-change rescan by TITAN SCOUT — finding must no longer appear.
5. Close ticket with Successful close_code.
```

Risk & Impact Analysis

```
Risk level: HIGH business risk — active exposure; fix required immediately.
Business impact if unremediated: Potential data exfil, privilege escalation, or compliance breach.
Scope: single resource (nsg-titan-webtier).
Blast radius: change is idempotent; pre-change snapshot captured by TITAN; auto-rollback available
if rescan fails.
Finding detail: NSG rule AllowSSHAll permits SSH (port 22) from 0.0.0.0/0 — Internet-wide
privilege escalation path to every VM in the subnet.
```

Backout / Rollback Plan

```
1. TITAN auto-captured snapshot of nsg-titan-webtier before change (baseline:
titan-live-demo-20260421T213642Z).
2. If post-change rescan still shows the finding OR a new issue appears within 15 min:
a. TITAN FORGE fires rollback automatically using stored snapshot.
b. Incident reopens and escalates to on-call.
3. Manual rollback command path (human override) is documented in close notes.
```

Test Plan

```
1. TITAN SCOUT rescans nsg-titan-webtier immediately after FORGE applies the change.
2. PASS criteria: the specific finding no longer appears in SCOUT results.
3. PASS criteria: no new CRITICAL or HIGH findings introduced by the change.
```

```
4. Automated compliance check: HIPAA/PCI/SOC2 controls re-evaluated.
5. If any check fails, backout plan fires automatically.
```

Recommended Fix Command

```
az network nsg rule update --name AllowSSHAll --nsg-name nsg-titan-webtier --resource-group
rg-titan-demo --source-address-prefixes VirtualNetwork
```

Compliance Mapping

```
CIS 1.x IAM, NIST AC-2, SOC 2 CC6.1, CIS Azure 6.2
```

AI Close Notes

```
(empty)
```