==========

INCIDENT RESPONSE REPORT

INC-2025-001: Unauthorized Privilege Escalation

==========

SECTION 1: EXECUTIVE SUMMARY

==========

On November 19, 2025, unauthorized privilege escalation was detected on Windows workstation MR-CHANDAN-PRAS. User account "mrhacker.indian@outlook.com" was granted nine dangerous system privileges without authorization. Wazuh monitoring detected this in real-time. Immediate actions taken: privileges revoked, account disabled, system isolated. No confirmed data breach. Incident escalated to Tier 2 for investigation. Recommendation: System rebuild and privilege access management implementation.

SECTION 2: TIMELINE

==========

16:02:42 UTC – Account modification detected (Event ID 4738)

16:02:42 UTC – Special privileges assigned (Event ID 4672)

├─ SeDebugPrivilege

├─ SeLoadDriverPrivilege

├─ SeImpersonatePrivilege

├─ SeTakeOwnershipPrivilege

├─ SeBackupPrivilege

├─ SeRestorePrivilege

├─ SeSecurityPrivilege

├─ SeSystemEnvironmentPrivilege

└─ SeDelegateSessionUserImpersonatePrivilege

16:02:43 UTC – Wazuh alert triggered

16:02:50 UTC – SOC team alerted

16:05:00 UTC – Incident investigation started

16:30:00 UTC – Tier 2 escalation email sent

17:00:00 UTC – Forensic analysis commenced

SECTION 3: IMPACT ANALYSIS

==========

System Impact: HIGH

• Workstation compromised

• Administrative privileges escalated

• System integrity compromised

• Lateral movement risk: HIGH

Data Impact: MEDIUM (No confirmed exfiltration)

• Risk of unauthorized data access

• Potential for data exfiltration

• User files at risk

• System files at risk

Operational Impact: MEDIUM

• Workstation offline for 4-6 hours

• User productivity impacted

• Department productivity affected

• System rebuild required

Compliance Impact: HIGH

• Policy violation: Unauthorized privilege escalation

• Access control violation

• Administrative procedures violated

• Audit trail compromised

Business Impact: MEDIUM

• Single workstation affected

• Estimated cost: $5,000-$10,000 (investigation + remediation)

• Reputation impact: LOW

• Customer impact: NONE

SECTION 4: REMEDIATION STEPS

==========

IMMEDIATE (Completed):

✓ Revoked all unauthorized privileges

✓ Disabled affected user accounts

✓ Isolated workstation from network

✓ Preserved forensic evidence

✓ Created incident ticket

SHORT-TERM (24-48 hours):

⧖ Complete forensic analysis

⧖ Full malware scan

⧖ System rebuild from clean backup

⧖ Reset administrator passwords

⧖ Verify no lateral movement

MEDIUM-TERM (1 week):

○ Deploy Privileged Access Management (PAM)

○ Implement privilege approval workflow

○ Enable real-time privilege monitoring

○ Conduct privilege audit

○ Security awareness training

LONG-TERM (Ongoing):

○ Implement zero-trust access model

○ Deploy Advanced Endpoint Detection (EDR)

○ Quarterly privilege audits

○ Regular incident response drills

○ Continuous monitoring and improvement

SECTION 5: LESSONS LEARNED

==========

What Worked:

✓ Real-time Wazuh detection caught threat immediately

✓ Rapid response prevented further compromise

✓ Good evidence preservation

✓ Clear escalation procedures

✓ Excellent documentation

What Failed:

✗ Weak privilege management controls

✗ No approval workflow enforcement

✗ Insufficient privilege monitoring

✗ Weak administrative access controls

✗ No automated response capabilities

Key Improvements Needed:

1. Implement Privileged Access Management (PAM)
2. Enforce mandatory approval for privilege changes
3. Deploy real-time privilege monitoring
4. Implement multi-factor authentication (MFA)
5. Enhanced endpoint detection and response (EDR)
6. Create automated incident response playbooks
7. Regular security training for administrators
8. Quarterly privilege access audits

Prevention Measures:

• Principle of least privilege enforcement

• Mandatory approval workflow

• Real-time monitoring of privileges

• Automated alerts on privilege changes

• Regular privilege reviews

- Separation of duties implementation
- Continuous logging and audit trails

==========