CIRT Playbook Battle Card: **GSPBC-1023 - Privilege Escalation - Exploitation for Privilege Escalation**

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Ensure antivirus/endpoint protection software is installed on workstations and laptops
4. Ensure that servers and workstations are logging to a central location
5. Make use of application sandboxing
6. Make use of exploit mitigation tools such as Windows Defender Exploit Guard
7. Ensure that good patch management practices are being followed

(I) Identification

1. Monitor for:
   a. Unusual DNS activity
   b. Antivirus/Endpoint alerts
   c. IDS/IPS alerts
2. Activity preceding and following escalation attempts may produce detectable IOC
3. Investigate and clear ALL alerts associated with the impacted assets

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Remove the affected system from the network
5. Determine the source and pathway of the attack
6. Issue a perimeter enforcement for known threat actor locations

(E) Eradication

1. Close the attack vector
2. Create forensic backups of affected systems
3. Perform endpoint/AV scans on affected systems
4. Reset any compromised passwords
5. Review the logs of all impacted assets
6. Patch asset vulnerabilities

(R) Recovery

1. Restore to the RPO within the RTO
2. Assess and address collateral damage
3. Determine the root cause of the incident
4. Resolve any related security incidents
5. Restore affected systems to their last clean backup

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals

Notes:

1. Report cybercrime: https://www.ic3.gov/default.aspx

GUARDSIGHT