

CIRT Playbook Battle Card: **GSPBC-1053 - Initial Access - Exploit Public-Facing Application**

(P) Preparation	(I) Identification	(C) Containment
<ol style="list-style-type: none">1. Patch asset vulnerabilities2. Perform routine inspections of controls/weapons3. Ensure antivirus/endpoint protection software is installed on workstations and laptops4. Confirm that servers and workstations are logging to a central location5. Review firewall, IDS, and IPS rules routinely and update based on the needs of the environment6. Conduct employee security awareness training7. Restrict users to the least privileges required8. Implement Web Application Firewalls (WAFs) ^[1]9. Segment externally facing servers and services from the rest of the network with a DMZ or by using separate hosting infrastructure ^[2]	<ol style="list-style-type: none">1. Monitor by:<ol style="list-style-type: none">a. Using deep packet inspection to look for artifacts of common exploit traffic, such as SQL injection strings, known payloads, and other indicators of compromise ^[3]2. Investigate and clear ALL alerts associated with the impacted assets3. Routinely check firewall, IDS, IPS, and SIEM logs for any unusual activity	<ol style="list-style-type: none">1. Inventory (enumerate & assess)2. Detect Deny Disrupt Degrade Deceive Destroy3. Observe -> Orient -> Decide -> Act4. Issue perimeter enforcement for known threat actor locations5. Archive scanning related artifacts such as IP addresses, user agents, and requests6. Determine the source and pathway of the attack
(E) Eradication	(R) Recovery	(L) Lessons/Opportunities
<ol style="list-style-type: none">1. Close the attack vector by applying the Preparation steps listed above2. Perform endpoint/AV scans on targeted systems3. Reset any compromised passwords4. Inspect ALL assets and user activity for IOC consistent with the attack profile5. Inspect backups for IOC consistent with the attack profile PRIOR to system recovery6. Patch asset vulnerabilities7. Reset accounts that have been breached immediately8. Remove any unapproved removable media from the environment	<ol style="list-style-type: none">1. Restore to the RPO (Recovery Point Objective) within the RTO (Recovery Time Objective)2. Address any collateral damage by assessing exposed technologies3. Resolve any related security incidents4. Restore affected systems to their last clean backup	<ol style="list-style-type: none">1. Perform routine cyber hygiene due diligence2. Engage external cybersecurity-as-a-service providers and response professionals3. Implement policy changes to reduce future risk4. Utilize newly obtained threat signatures5. Remember that data and events should not be viewed in isolation but as part of a chain of behavior that could lead to other activities <div>References:<ol style="list-style-type: none">1. MITRE ATT&CK Mitigation M1050: https://attack.mitre.org/mitigations/M1050/2. MITRE ATT&CK Mitigation M1030: https://attack.mitre.org/mitigations/M1030/3. MITRE ATT&CK Data Source DS0029: https://attack.mitre.org/datasources/DS0029/</div>

Resources:

- GuardSight GSVSOC Incident Response Plan: https://github.com/guardsight/gsvsoc_cybersecurity-incident-response-plan
- IT Disaster Recovery Planning: <https://www.ready.gov/it-disaster-recovery-plan>
- Report Cybercrime: <https://www.ic3.gov/Home/FAQ>