**CCDC 2020 Security Incident Report**

|  |  |
| --- | --- |
| 1. Contact Information | |
| Team Number: |  |

|  |  |  |  |
| --- | --- | --- | --- |
| 1. Incident Description (Check all that apply) | | | |
|  | Account Compromised |  | Social Engineering |
|  | Denial of Service |  | Technical Vulnerability (0-day Attacks) |
|  | Malicious Code (Virus, Malware) |  | Theft/Loss of Proprietary Property/Media |
|  | Misuse of Systems |  | Unauthorized Access |
|  | Reconnaissance (probes, scans) |  | Unknown/Other |
| *Description of Incident:* | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| 1. Scope of Incident (Check One) | | | |
| *NOTE: Critical and High scope incidents must be made known by all tech employees via phone calls, emails, meetings, and other various methods of communication.* | | | |
|  | **Critical** – affects public safety or state-wide information resources | | |
|  | **High** – affects company’s entire network, namely critical business practices | | |
|  | **Medium** – affects company infrastructure, such as servers or admin accounts | | |
|  | **Low** – affects company workstations or user-level experiences | | |
|  | **Unknown/Other** | | |
| Estimated number of affected systems: | | |  |
| Estimated number of users affected: | | |  |
| Third Party Members involved/affected (if any) | |  | |
| *Additional Scope Information:* | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| 1. Impact Analysis (Check all that apply) | | | |
|  | Loss of Access to Services |  | Propagation to Other Networks (list below) |
|  | Loss of Productivity |  | Unauthorized Disclosure of data/info |
|  | Loss of Reputation |  | Unauthorized Modification of data/info |
|  | Loss of Revenue |  | Unknown/Other (describe below) |
| *Additional Information:* | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| 1. Sensitivity of Affected Information (check all that apply) | | | |
|  | Confidendial/Sensitive Data |  | Personally Identifiable Information (PII) |
|  | Critical Infrastructure Information |  | Financial Data |
|  | Non-Sensitive Data |  | Intellectual Property/Copyrighted Info |
|  | Publicly Available Data |  | Unknown/Other |
| *Additional Details:* | | | |

|  |  |
| --- | --- |
| 1. Remediation of Incident | |
| What actions did you take to identify the affected resources in the incident? |  |
| What actions did you take to mitigate the damage and remediate the incident? |  |
| What do you propose the company does differently to prevent this from happening in the future? |  |
| *Additional Comments/Points of Discussion:* | |

|  |
| --- |
| 1. Miscellaneous – provide any other pertinent information here |
|  |