**IR Report**

|  |  |
| --- | --- |
| **Affected Host** | [*Hostname, i.e. Ecom*] |
| **Source IP Address** | [*Attacker IP*] |
| **Destination IP Address** | [*Host IP*] |
| **Port and Service** | [*Relevant Port, i.e. TCP 80 - HTTP*] |
| **Initial Access Timestamp** | [*Time, i.e. 10:12am CT*] |
| **Service Downtime** | [*Time range service was down*] |
| **Remediated Timestamp** | [*Time when service restored*] |
| **Affected Account** | [*Account name*] |

## Executive Summary

[*Provide an overview that is clear and concise. What has our team identified?*]

## Vulnerability

### Explanation

[*Technical details, what was found, where was it, what is vulnerable*]

### Evidence

|  |
| --- |
| [*Copy/Paste terminal text, filenames, directories, logs, etc here*] |

## Initial Access

### Explanation

[*Method of compromise, cause, etc*]

### Evidence

|  |
| --- |
| [*Copy/Paste terminal text, filenames, directories, logs, etc here*] |

## Impact

### Explanation

[*Brief summary of incident, what happened, how this affects us*]

### Evidence

|  |
| --- |
| [*Copy/Paste terminal text, filenames, directories, logs, etc here*] |

## Eradication

### Explanation

[*What we did. Keep short and brief, put details in REMEDIATION section*]

### Evidence

|  |
| --- |
| [*Copy/Paste terminal text, filenames, directories, logs, etc here*] |

## Remediation

### Explanation

[*Steps taken to address the problem*]

### Evidence

|  |
| --- |
| [*Copy/Paste terminal text, filenames, directories, logs, etc here*] |

Respectfully,

Team #