**Incident Report**

**Team 17**

**February 13, 2025**

# **1. Executive Summary**

**Incident ID:** INC-2025-02-13-XX

**Incident Priority:**

P1 - Critical P2 – High P3 - Medium P4 - Low

**Incident Classification:**

Compromised System

Compromised User Credentials

Network Attack (e.g., DoS)

Malware (e.g., virus, worm, Trojan)

Reconnaissance (e.g., scanning, sniﬃng)

Lost Equipment/Theft

Physical Break-in

Social Engineering (e.g., phishing)

Policy Violation (e.g., acceptable use)

Other:

**Incident Summary:**

On February 13, 2025 at [time], Team 17 detected [incident]. Using [methods], an unauthorized entity [action (ex. gained access to, compromised, exfiltrated)], impacting [impacted assets].

# **2. Incident Detection & Analysis**

**2.1. Aﬀected Systems & Data**

The following is a list of system(s) impacted by the incident, along with the data on or accessible by the aﬀected systems (NIST CSF DE.AE-04) [[1]](#footnote-2).

Click or tap here to enter text.

The following is a list of user(s) impacted by the incident, including system access levels and privileges (NIST CSF DE.AE-04).

Click or tap here to enter text.

**2.2. Indicators of Compromise (IoCs)**

This section lists the key pieces of evidence used to determine that an attack has occurred (NIST CSF DE.AE-08).

Click or tap here to enter text.

**2.3. Root Cause Analysis**

This section explains the primary factors that enabled the incident to occur (NIST CSF RS.AN-03).

Click or tap here to enter text.

**2.4. Incident Classification & Priority**

Based on the findings from the investigations, an incident is given an incident priority and classification to help guide and activate response efforts (NIST CSF RS.MA-03).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Incident Priority**  **Matrix** | | **Impact** | | |
| **High**  Business-critical systems OR multiple departments and customers OR business-critical data is impacted. | **Medium**  Non-business-critical systems are impacted AND one department or multiple customers are affected. | **Low**  Non-business-critical systems are impacted. Partial department, or one customer is impacted. |
| **Urgency** | **High**  Causes immediate and significant disruption affecting critical business functions, security or safely. | **P1 - Critical** | **P2 - High** | **P3 - Medium** |
| **Medium**  Causes immediate and moderate disruption but no critical business functions affected. Workaround may be available. | **P2 - High** | **P3 - Medium** | **P4 - Low** |
| **Low**  Will cause disruption soon if not addressed. Workaround is available. | **P3 - Medium** | **P4 - Low** | **P4 - Low** |

With an impact score of [High, Medium, Low] and an urgency score of [High, Medium, Low], this incident is given [P1, P2, P3, P4] priority. The incident is classified as [look at classifications on page 1].

# **3. Response and Recovery Analysis**

This section describes:

1. the immediate response to contain the threat and prevent further damage upon incident identification, such as disabling user accounts, resetting credentials, and isolating devices (NIST CSF RS.MI-01).
2. the steps taken to patch vulnerabilities and eradicate any malware, backdoors, persistence methods, and other things left by the threat actor (NIST CSF RS.MI-02).
3. outlines the steps taken to validate, rebuild, and restore data and systems to normal operation after verifying the eradication of the threat (NIST CSF RC.RP).

Click or tap here to enter text.

# **4. Recommendations**

The following lists recommendations related to:

1. users and personnel, such as security awareness training and staffing (NIST CSF PR.AT).
2. policies, procedures and processes for improving incident prevention and response (NIST CSF GV.PO, ID.IM).
3. technology solutions for improving organizational security posture against threats.

Click or tap here to enter text.

# **Appendix: Technical Timeline**

| **Date & Time** | **Activity** |
| --- | --- |
| 2/13/2025 HH:MM |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

1. The NIST Cybersecurity Framework (CSF) 2.0 (https://doi.org/10.6028/NIST.CSWP.29) [↑](#footnote-ref-2)