NCSA Incident Response Policy

Document Name: NCSA Incident Response Policy
Version: 1.1
Accountable: Alex Withers
Authors: Adam Slagell, Alex Withers

Reviewed: June 23, 2021
Approved: June 22, 2020

Introduction

This document represents the policies and procedures in place for handling information security incidents impacting services and infrastructure of the National Center for Supercomputing Applications (NCSA) and associated projects. This includes publicly available services, supporting information and information systems, and infrastructure used byNCSA personnel in support of NCSA and associated projects.

For the purpose of this document, an information security incident (henceforth an "*incident*") includes any known or suspected event that compromises or has the potential to compromise any NCSA information asset, including computing infrastructure, confidential data, or computing service, as well as flagrant violations of NCSA policy by project personnel, staff, or users of externally-facing services. Incident that do not involve information assets fall outside of the scope of this document.

Goals

In order to guide time-sensitive tactical decisions we use the following goals in decreasing order:

1. Minimize negative impact from an incident in terms of exposing confidential information, damage to hardware, software, and/or data assets, and damage to NCSA reputation.
2. Collect information needed
    a. to understand the specific impact the incident had on impacted assets
    b. to prevent future incidents
    c. when appropriate, to give law enforcement data useful in pursing investigation of crimes related to the incident
3. Keep NCSA leadership and stakeholders informed.
4. Maintain the operational availability of systems, services, and infrastructure to their users.

These priorities may be adjusted as warranted.

Preparations in Place

Roles and Responsibilities

- IRST - Incident Response and Security Team
- TL - IRST Team Lead

- IRL - Incident Response Lead
- TM - IRST Team Member
- CISO - Chief Information Security Officer
    - Note: Some projects have an ISO (Information Security Officer) instead of a CISO. These roles are treated the same within the context of this document.
- DO - Directors Office
- U of I Campus CISO - The Chief Information Security Officer of the University of Illinois, see https://techservices.illinois.edu/security
- HIPAA Privacy Officer - The U of I system HIPAA Security and Privacy Officer, see https://hipaa.uillinois.edu/contact/

Role	Responsible Person	Description
Initial Responder	IRL/TM	Initial Responder assesses an incident and coordinates response. For non-critical issues most IRST members will follow standard procedures. For unique or critical issues the IRL will determine the appropriate course of action.
Communications	TL	The TL or designate will coordinate timely communication with the DO and CISO as situations develop for issues that warrant such notification. The TL or designate will also update the all appropriate communications paths for notifying NCSA users.

Escalation Paths

Signs of an incident primarily come from IRST monitoring. Other sources of notification could come from:

- System or service owners;
- Data owners;
- Ticketing system;
- Communication from an affected user via phone, instant message, or face-to-face communication;
- Incident notification through trusted third parties such as REN-ISAC.

The IRST will make a determination as to whether these events and indicators constitute an incident. The IRST will trigger this incident response policy if it determines that the events and indicators do indeed constitute an incident. The severity classifcation and corresponding actions are discussed below.

It is a required that any significant NCSA projects have a point of contact for coordinating security incidents and that this information, including appropriate methods of communication and expected availability, be maintained by both the project and IRST. In cases where a project contact is not specified the assumed contact is the project's Principle Investigator (PI).

Any incidents that need to be reported to the IRST should be done initially through the ticketing system either directly through the ticketing system interface or via email at the following email address: help+security@ncsa.illinois.edu. This is to ensure that progress on an incident is tracked through a ticket. If the ticketing system is unavailable the NCSA Help Desk should be contacted to relay information to the appropriate personnel.

Response Procedure Testing

Response procedures can not be considered reliable unless they are regularly tested. The first application of an incident response procedure should not be in the heat of an actual incident, however, it will likely occur if new procedures must be developed on the fly.

Procedures dealing with common events should be tested on a regular bases especially when the infrastructure for which this tool either relies on or affects changes. The IRST should have test accounts in all appropriate systems to evaluate the effectiveness of these procedures.

On most occasions these tests should be unannounced and the response times should be recorded for review.

The following non-exhaustive list of procedures should be tested:

- User account disabling
- Password resets
- User/Host identification
- Host blocking
- Firewall changes
- ⚠️

External Documentation

NCSA IRST will maintain the following on an ongoing basis in order to facilitate response to an incident. Some of these must be maintained by other parties within NCSA.

- Bro Logging
- Syslog Collection
- Log Storage for a period of 1 year
- Security Contacts for individual systems or networks - This is performed by Network Engineer contact information.
- Asset inventory detailing all IT assets - Performed by NCSA inventory tracking system
- Communications Blog for end-user communication of security issues
- ⚠️

General Procedures

IRST Procedures

The IRST team maintains procedures for incident handling: IRST - Incident Response Procedures. This document provides specific instructions and procedures for IRST.

Identify

All security alerts should be tracked through the NCSA Ticketing system, JIRA, specifically in the HELP+SECURITY queue. This can be done through logging in directly to JIRA or by sending an email to help+security@ncsa.illinois.edu.

For incidents that require IMMEDIATE attentions contact an IRST TM directly or contact the NCSA Help Desk.

Issues that affect individual projects but not NCSA directly should be reported to the PI of that project.

Incidents may include, but are not limited to:

- Unauthorized access to systems or services;
- Unauthorized deployment of applications on systems or services;
- Unauthorized exfiltration of data from systems or services;
- Large scale probing, scanning, and/or credential stuffing attacks against services;
- Attacks originating from within the organization.

The IRST team will use its judgement to determine whether events necessitate a triggering of this incident response policy.

Assess and Preserve

Initial Triage and Categorization

Information security incidents are classified based on their perceived impact. A classification should be determined as quickly and carefully as possible and classification may change as understanding of the incident improves. The first person to respond to the incident should attempt to give a first-estimate categorization in order to guide response. The following classifications are based on NIST 800-61 section 3.2.6.

High: an incident is considered High Severity if it involves:

- Compromise of confidentiality or integrity of PII
- Compromise of confidentiality or integrity of a password database
- Compromise of confidentiality or integrity of software vulnerability information
- Attention by media outlets, or other public dissemination (e.g. social media)
- Major disruption to the project's ability to provide services to the user community
- A successful compromise is believed to have been ongoing for more than a week
- An incident is believed to have possible financial consequences
- An incident is believed to involve an insider threat

Medium: an incident is considered Medium Severity if it involves:

- Disruption to the project's ability to provide services to multiple users for an extended time (more than 10 minutes)
- Compromise of multiple user's accounts by the same party
- Any compromise that appears to specifically target this project's assets or personnel

Low: an incident is considered Low Severity if it involves:

- Disruption to a single user's ability to use the project's services (e.g. a compromised password that results in temporarily disabling the account)
- A short-term (less than 10 minute) disruption in the project's availability due to a denial of service attack
- A long-term disruption to non-critical services or degradation of critical services
- Attempted but unsuccessful attempts to compromise the project's infrastructure in some way that appears to target the project specifically and is not normal untargeted internet "background noise"

Based on this initial categorization, the following actions should be taken:

High Severity: Project and/or NCSA CISO and primary maintainer of the affected system(s) should be notified immediately. Notification should not be sent blind and attempts to contact a responsible party should continue until a response is confirmed.

Medium Severity: The project and/or NCSA CISO and primary maintainer of the affected system(s) should be notified by voice during business hours and email notification during off-hours.

Low Severity: Email notification should be sent to the project and/or NCSA CISO and primary maintainer of the affected system(s).

In all cases any compromised accounts should be disabled.

PHI data workflow

Incidents involving electronic Protected Health Information (ePHI) are a special case, which requires extra steps to be followed to guard against the flow of ePHI outside the NCSA Health care Component, i.e. the workforce members who are a part of the covered entity at NCSA.

Notifications

Any incidents that expose ePHI shall be reported to the NCSA CISO and HIPAA Liaison as soon as confirmation or reasonable inference of exposure is made. Subsequently they will contact University of Illinois and UIUC HIPAA officers.

Discussions regarding an incident involving ePHI will be limited to the parties mentioned above, those in the NCSA Health Care Component and other parts of the University of Illinois covered entity as necessary and authorized.

Incident investigation workflow

This applies to any systems with ePHI which are involved in an incident investigation or at anytime a breach is suspected.

1. The incident responder on the security team will setup an encrypted space either locally or shared with other incident response team members immediately. Any data collected or notes taken will be stored in this space, transferred to it over encrypted channels if it goes over the network. This could be a shared network volume, portable drive, local volume, or U of I's Box service cloud storage service.
2. The responder will need likely need assistance from the customer to determine the identities of any parties affected and the corresponding contact information necessary for breach notifications. This means a secure communication channel must be established for any data transferred. Each customer has a point of contact for any agreement or work, and the incident responder will work through that person, contacting by phone first, to find the appropriate personnel at the customer to work with on the investigation (This is assuming there are no established procedures for the customer). One of the first tasks will be to establish secure communication channels, e.g. encrypted email with verified keys, SFTP transfers, or approved cloud storage, such as, Box. In the case of a breach, we must coordinate through the university HIPAA officer before talking with a third party. The CISO is responsible for working with the HIPAA liaison to coordinate this engagement.
3. Incident reports for consumption outside of the security team will be sanitized as not to contain any actual ePHI. This level of detail is not needed for management. University HIPAA officers and security team members can request more detailed information either through the NCSA CISO or HIPAA liaison. Such information be transferred through University approved methods like Box, or on encrypted portable media.
4. Once it is determined who must be notified, NCSA senior leadership will decide whether we do notification in-house or out of house. They do not need to know any names, just the number of individuals and what kind of data was exposed, e.g. names, DOB, images, etc. The breach letter itself will be worked on with the HIPAA Officer and the campus Legal.
    a. If we go with a third party, NCSA will follow the recommendation of the U of I HIPAA officer or UIUC liaison most likely. Secure channels of communication will need to be setup with them to give the contact info.
    b. For a small breach, we may handle mailing the letters in-house. In this case an incident responder will give an NCSA clerical who is within the covered entity the letter and list of exposed persons with contact information. This list will be transferred to the clerical through either an approved University solution, such as Box, or via encrypted flash drives.
5. Long term archives of investigation, not including the sanitized report, will be stored on encrypted volumes accessible only by NCSA security team members and the NCSA CISO.

It is assumed that any such incident happens on server in the Advanced Computational Healthcare Enclave. If PHI was removed from this system be workforce members outside of the breach workflow above for an incident investigation, then workforce members broke multiple University and NCSA policies and disciplinary action will be in order. We will work with the UIUC HIPAA liaison, NCSA human resource, and NCSa senior management to decide how best to address such a serious policy violation.

Isolation

In any incident, it is important to act quickly in order to keep damage from spreading. Before or in parallel with the formation of an incident response team (when required), the person doing initial triage should take steps to prevent the problem from spreading to other accounts or resources. This includes isolating systems by blackhole routing the host, switch port disable, or physical disconnection from the network.

Formation of the Incident Response Team

The IRL may form an incident response team. The composition of the team will depend on the nature of the incident and may evolve over time. IRT members may include individuals outside of the security group that have specialized skills and/or knowledge of the affected system(s).

Information Capture

Information capture during an incident is essential to fast and appropriate resolution of the incident, as well as to understanding the incident's cause, working with law enforcement regarding the incident, and doing an effective postmortem. Members of the incident response team should log their actions, on paper if needed to isolate record-keeping from potentially compromised assets, along with times and observations made. Additionally, team members must, whenever possible, keep copies of malicious software found, and other signs of compromise for later analysis. Efforts should be taken to keep affected systems powered on should volatile forensic evidence need to be collected.

Eradicate and Recover

Once an incident is contained and all evidence is collected, the IRL will provide the all-clear to restore services of the affected host.

Eradication

A compromised host ideally should be rebuilt from scratch ensuring that all security updates and applied. Any outstanding vulnerabilities that are not patched, especially those that were used to compromise the host initially, should be mitigated. If mitigation of a current vulnerability is not possible the host should not be returned to service without the expressed risk-acceptance of the system/service administrator, the CISO of the project and the CISO of NCSA.

If a host can not be rebuilt from scratch, the host will need to be patched and go through a vetting by the security team to determine if there are any backdoors or other potential vulnerabilities. The host will not be allowed onto the network until there is risk-acceptance by the system/service administrator, the CISO of the project and the CISO of NCSA.

Recovery

Once a system/service is restored, including restoration of data from backups, an assessment of the host should be performed to ensure that the initial threat vector used to compromise the system/service is patched/mitigated.

Notification

The NCSA CISO is responsible for reporting any incidents to external parties outside of NCSA. The IRL is responsible for reporting incidents to the CISO and the Director's Office.

- If theft of University property is involved, a police report should be filed with campus police. This process should be handled through NCSA shipping and receiving.
- Any incidents that affect the reputation of the Center or the University should be reported to the Office of Public Affairs.
- Any incidents involving identity theft or incidents that involve over $1000 in real damages should be reported to the local FBI field office.
- Violations of HIPAA or any other regulatory policies are to be reported as those policies dictate.
    - Security and Confidentiality incidents related to the ACHE environment should be reported to the HIPAA Privacy Officer and the U of I campus CISO. Evidence of this communication should be retained.

Please see the contact procedures for external partners: NCSA Security Contact Process.

Follow Up and Lessons Learned

Following an incident, any issues identified during the incident response process should be reviewed. Existing processes should be checked for accuracy and should be updated as necessary. It is recommended that a formal meeting occur to verbally review the incident to ensure that nothing was missed and all relevant information is recorded.