Computer Security Incident Response Team

REN-ISAC Computer Security Incident Response Team (CSIRT) is staffed 24x7 to receive and disseminate timely information regarding cybersecurity incidents in the higher education community. The CSIRT will receive, analyze, and escalate reports concerning sources and victims of attacks and respond to inquiries concerning network-based threat.

RFC2350 Description

1. About this document

1.1 Date of Last Update
Version 1.04, published 2020-10-29

1.2 Distribution List for Notifications
E-mail notification of updates are sent to: ren-isac-info@lists.ren-isac.net. Subscription requests for this mailing list should be sent to soc@ren-isac.net.

1.3 Locations where this Document May Be Found
The current version of this CSIRT description document is maintained at
https://www.ren-isac.net/services/csirt.html

1.4 Authenticating this Document
A version of this document signed with the REN-ISAC team PGP key is available at
https://www.ren-isac.net/services/CSIRT_RFC_2350.pdf.asc

2. Contact Information

2.1 Name of the Team
REN-ISAC (Research & Education Networks Information Sharing & Analysis Center)

2.2 Address
REN-ISAC
2715 E. 10th Street
Bloomington, IN 47408
USA

2.3 Time Zone
US/Eastern: GMT-0500, and GMT-0400 Daylight Time (observation dates)

2.4 Telephone Number
+1 317 274 7228

2.5 Facsimile Number
+1 812 856 0253 - be advised, this is not a secure fax.

2.6 Other Telecommunication
None available.

2.7 Electronic Mail Address
soc@ren-isac.net

2.8 Public Keys and Other Encryption Information
The REN-ISAC PGP key has the KeyId 0x4DFD37BE and is also accessible at http://pgp.mit.edu/.

2.9 Team Members
Information about team members is maintained on the REN-ISAC staff page.

2.10 Other Information
General information is available at the REN-ISAC public webpage.

2.11 Points of Customer Contact
The preferred method for contacting REN-ISAC is via e-mail to soc@ren-isac.net.

Please sign your messages using your own PGP key, accessible at public key servers; and use PGP encryption when sending sensitive information (section 2.8).

In addition you can contact REN-ISAC by phone (section 2.4).

Emergency communications must clearly state EMERGENCY or URGENT in an e-mail subject or the initial phone contact.

Normal hours of operation are 0800 to 1700 U.S. Eastern; however, the 24x7 Watch Desk will respond to emergencies outside of normal business hours.

End users are expected to contact their local IT support for assistance. In most cases only limited support will be provided by REN-ISAC directly to end users. REN-ISAC's preferred point for engagement is with persons who have organization-wide responsibility for security protection and response.

All communications are conducted in English.

3. Charter

3.1 Mission Statement
The REN-ISAC mission is to aid and promote cybersecurity operational protection and response within the research and higher education (R&E) communities. The mission is conducted through private information sharing within a community of trusted representatives at member organizations, and as a computer security incident response team (CSIRT) supporting the R&E community at-large. REN-ISAC serves as R&E's trusted partner in commercial, governmental

and private information sharing relationships, in the formal U.S. ISAC community, and for served networks.

3.2 Constituency
The REN-ISAC CSIRT's constituency includes U.S. and Canadian higher education and research (R&E) institutions, U.S.-based state, national, and global R&E networks, and organizations within the .edu top-level domain. (Note: this differs from the REN-ISAC trust community constituency which includes the "Five Eyes" countries AU,CA,NZ,UK,US.)

3.3 Sponsorship and/or Affiliation
The REN-ISAC is hosted at Indiana University. It receives funding and support from membership fees, Indiana University, Louisiana State University, Internet2, and EDUCAUSE. Affiliations are maintained with various private, commercial, and governmental security information sharing organizations and activities.

3.4 Authority
REN-ISAC coordinates security incidents on behalf of our constituency and at our constituents request.

Authority was established by agreement with the National Infrastructure Protection Center (NIPC) in 2003 and subsequently affirmed through the EDUCAUSE and Internet2 Higher Education Information Security Council.

Concerning its broad constituency, the REN-ISAC CSIRT's main purpose in incident handling is the coordination of incident response. As such, we advise only and have no authority to require or execute actions.

4. Policies

4.1 Types of Incidents and Level of Support
REN-ISAC responds to all types of cybersecurity incidents and threat within its constituency (section 3.2). The nature and level of engagement depends on the type and severity of the incident or threat, the breadth of affected parties, and our resources at the time.

All incidents are considered normal priority unless communicated as URGENT or EMERGENCY. If you have an urgent issue, when reaching out to our Points of Contact (section 2) by e-mail, state URGENT or EMERGENCY in the subject line; if by phone, state one of those keywords in the initial contact.

For normal priority reports, contact by e-mail is preferred. Our service level objectives are to have a human-provided acknowledgement within four normal business hours and a response within 24 hours.

End users are expected to contact their local IT support for assistance. In most cases only limited support will be provided by REN-ISAC directly to end users. REN-ISAC's preferred point for engagement is with persons who have organization-wide responsibility for security protection

and response.

4.2 Cooperation, Interaction and Disclosure of Information

REN-ISAC interacts with private, commercial and governmental organizations in the course of sharing information concerning active threats, incidents, and vulnerabilities. REN-ISAC limits disclosure of incident information to affected parties and other entities authorized by the parties. No information concerning sources or methods will be shared unless explicit permission is received and is necessary for response.

REN-ISAC supports use of the Information Sharing Traffic Light Protocol. Information tagged with TLP will be handled accordingly.

When sharing information to REN-ISAC, organizations should be cognizant of relevant laws, regulations, and standards concerning information disclosure (e.g. FERPA, HIPAA, PCI DSS, etc).

4.3 Communication and Authentication

For normal communication not containing sensitive information REN-ISAC uses conventional methods such as unencrypted e-mail or telephone.

For sensitive communications PGP encrypted e-mail and encrypted files are preferred, however conventional telephone is also supported. If it is necessary to authenticate the identity of a person before communicating, this will be done through existing webs of trust, or organizational charts and documentation on organizational web sites.

The use of an institutional e-mail address is recommended and in cases of sensitive data exchange may be required.

5. Services

5.1 Incident Response

REN-ISAC will assist information security staff, system and network administrators as well as management in handling the technical and organizational aspects of incidents. In particular, it will provide assistance or advice with respect to the following aspects of incident management:

5.1.1 Incident Triage

- Understanding whether indeed an incident occurred.
- Assessing and prioritizing the incident.

5.1.2 Incident Coordination

- Determining the involved organizations.
- Contacting the involved organizations to investigate the incident and take the appropriate steps.
- Facilitating contact to other parties which can help resolve the incident.
- Facilitating contact with law enforcement.
- Sending reports to other CSIRTs.

5.1.3 Incident Resolution
- Advising on appropriate actions.
- Advising on mitigation techniques.

REN-ISAC may collect statistics about incidents within its constituency.

5.2 Proactive Activities
- Work with global remediation communities to identify security threats.
- Send security notifications to our constituents.
- Maintain a database of networks, sites and security contacts.
- Publish announcements and alerts concerning security threats.
- Raise security awareness in its constituency.
- Use scanners to detect vulnerable systems and/or services.
- Conduct periodic web seminars on computer security-related topics; these web seminars are generally limited to REN-ISAC members; however, some are open to the public.

6. Incident Reporting Forms

Please report security incidents via e-mail or phone to the points of contact described in section 2 of this document. Reports by e-mail to soc@ren-isac.net will be acknowledged within four normal business hours by a human (normal priority incidents). Because e-mail is an imperfect means of communication (susceptible to filtering, stripping, time delay, etc.) if you don't receive an expected response, please follow-up by phone.

If the matter is urgent, place URGENT or EMERGENCY in the e-mail subject, and/or use our phone Point of Contact (section 2).

Incident reports should contain the following information:

Incident description.
Desired action(s).
Incident timestamps (including time zone). Are the timestamps NTP synchronized or otherwise trustworthy?
All relevant Internet identifiers (e.g. source and destination IP addresses, ports, and protocols; URLs, e-mail addresses, host names, etc.). Note that source port is particularly important to include because of NAT.
Relevant log and/or monitoring (NetFlow, pcap, etc.) files, in commonly-used formats.

MIME attachments are accepted.

When suitable, bulk incident data should be reported in the Team Cymru "ASN format."

7. Disclaimers

Information is shared by REN-ISAC for the objective of cybersecurity protection and response. Information is shared in good faith and there are no explicit or implied guarantees or warranties

to the veracity or applicability of the information.

Information received from any REN-ISAC service or product must be analyzed fully by representatives of the receiving institution, and inherent risks determined and understood. Any local action taken must be informed by local technical expertise and applied as appropriate to the local technical, functional, and cultural environments.

The REN-ISAC, its sponsoring organizations, and members accept no responsibility for negative impacts of any sort that results from local actions taken on information sent to the membership generally, or to specific institutions.