المركز الوطني الإرشادي
للأمن السيبراني
SAUDI CERT

RFC 2350

SAUDI CERT

1. Document Information

This document contains a description of Saudi CERT in according to RFC 2350.
It provides basic information about the Saudi CERT team, its channels of communication, its roles and responsibilities, and services provided by Saudi CERT.

1.1. Date of Last Update

Version 1.0, Created 08-06-2020
Version 2.0, Modified 29-08-2023

1.2. Distribution List for Notifications

Saudi CERT publishes two information products on its website and pushes one of them to each subscriber of Saudi CERT. By subscribing to Saudi CERT mailing list, users receive information about vulnerabilities and mitigations along with weekly newsletter that contains the latest security warnings/alerts and cybersecurity awareness materials uploaded to the website. You can subscribe by visiting the link below: https://cert.gov.sa/en/newsletter/?email=

1.3. Locations where this Document May Be Found

A current version of this RFC 2350 document is available on the Saudi CERT website: https://cert.gov.sa/en/about-us/

1.4. Authenticating this Document

This document has been signed with Saudi CERT PGP key.

2. Contact Information

2.1. Name of the Team

Full Name: Saudi Computer Emergency Response Team
Short Name: Saudi CERT

2.2. Address

National Cybersecurity Authority
Al Raidah Digital City - An Nakheel District
Al Mahir Street, Building No 6672, Unit No. 3
Riyadh 12382 - 4149
Kingdom of Saudi Arabia

2.3. Time Zone

GMT+3

2.4. Telephone Number

Within Saudi Arabia: 011 407 6366
From outside Saudi Arabia: +996 11 407 6366

2.5. Facsimile Number

None

2.6. Other Telecommunication

None

2.7. Electronic Mail Address

incidents@cert.gov.sa
info@cert.gov.sa

2.8. Public Keys and Encryption Information

Saudi CERT
Fingerprint: 9163F542F39E020C3246CBB9D8167DC14E98332B
https://cert.gov.sa/en/pgp-key/

2.9. Team Members

The team leader and the general manager of Saudi CERT and a full list of Saudi CERT's team members are not publicly available.
Management and supervision are provided by the Cybersecurity Technologies and Operations Sector, National Cybersecurity Authority (NCA).

2.10. Other Information

General information about Saudi CERT is available on the link below:
https://cert.gov.sa/en/about-us/

2.11. Points of Customer Contact

For operational inquiries: https://cert.gov.sa/en/report-vulnerability/

For general inquiries: https://cert.gov.sa/en/contact-us/

3. Charter

3.1. Mission Statement

Saudi CERT's primary mission is to raise cybersecurity awareness in the Kingdom of Saudi Arabia. Saudi CERT increases the level of knowledge and awareness regarding cybersecurity risks and attempts to mitigate their impact by issuing warnings about the latest and most dangerous vulnerabilities. Saudi CERT also launches awareness programs and campaigns and cooperates and collaborates with other response teams.
Saudi CERT aims to:

- Raise the level of awareness for citizens, private sector and national entities.
- Approve plans and establish advanced approaches to detect and analyze warnings, as well as to approve and constantly develop modern technologies.
- Issue warnings and share alerts to protect individuals and entities.
- Support the maintenance and maturity of the national cyber security posture.
- Encourage government and private organizations to build capabilities that have adequate cybersecurity knowledge, as well as developing cybersecurity knowledge for individuals by organizing events and workshops.
- Cooperate and build national and international partnerships.
- Participate in international events and conferences to exchange experiences and information.
- Learn the best practices regarding cybersecurity awareness and activate educational programs for different audience levels.
- Share best practices that help mitigate security vulnerabilities.

3.2. Constituency

Saudi CERT is the national CSIRT for Saudi Arabia. The constituency of Saudi CERT is composed of everyone is the kingdom; public and private sectors and the general public.
National CSIRTs located outside of Saudi Arabia, services may be provided to any of these entities as requested, depending on resource availability.

3.3. Sponsorship and/or Affiliation

Saudi CERT is part of the National Cybersecurity Authority (NCA), which is a government entity who is in charge of cybersecurity in Saudi Arabia and serves as the national authority on its affairs.

3.4. Authority

Saudi CERT operates as the governmental CSIRT under the authority of National Cybersecurity Authority (NCA) as its one of centers that belongs to NCA. Saudi CERT also strives to maintain active cooperation and partnerships with all the national CERTs.

4. Policies

4.1. Types of Incidents and Level of Support

Saudi CERT works as coordinator for mitigating the impacts of security incidents at an appropriate support level depending on the type, severity and extent of the incidents.

4.2. Co-operation, Interaction and Disclosure of Information

Saudi CERT classifies data and information in all forms. It intends to set the appropriate classification levels to apply the corresponding security measures and reduce the risk of protected information disclosure.

All incoming information is handled confidentially by Saudi CERT, regardless of its priority and level of classification. Information that is clearly sensitive in nature is only communicated and stored in a secure environment, if necessary using encryption technologies.

Saudi CERT exchanges information with the global CSIRT community to improve the security and facilitate a greater sharing of information by using Traffic Light Protocol (TLP).

4.3. Communication and Authentication

The preferred method of communication is via e-mail. When the content is sensitive enough or requires authentication, Saudi CERT's PGP key is used for signing. All sensitive communication to Saudi CERT shall be encrypted using the team's PGP key.

5. Services

1. Alerts and Warnings
2. Incident Response
3. Incident Response Coordination
4. Vulnerability analysis
5. Vulnerability response
6. Vulnerability response coordination
7. Announcements
8. Awareness building
9. Education/training

Saudi CERT's general services are summarized below:
- Warnings
- Reports

- Events
- Workshops
- Cyber awareness materials

Saudi CERT seeks to raise awareness levels for citizens and organizations by raising cybersecurity awareness. Saudi CERT provides services that facilitate;

- the management and release of cybersecurity alerts,
- cooperation with similar organizations,
- launching national programs that demonstrate the importance and dangers of cybersecurity,
- releasing cyber awareness materials that describe the most prominent risks and best practices to prevent and mitigate these risks to enhance national awareness.

These efforts will enable the cybersecurity community in the Kingdom of Saudi Arabia to become more resilient and agile when dealing with cybersecurity risks and attacks.

6. Incident Reporting Forms

To report an incident or vulnerability to Saudi CERT, please visit:
https://cert.gov.sa/en/report-vulnerability/

7. Disclaimers

The information in this document are provided on a "as is" basis. The National Cybersecurity Authority (NCA) does not guarantee the accuracy, adequacy or completeness of this information.

The National Cybersecurity Authority (NCA) expressly disclaims liability for any damage caused by error or inaccuracy in the information or any decision based on the information contained in this document.