RFC 2350 DESCRIPTION

for

BSS-CERT

CONTACT PERSON	COMPANY DETAILS
Andrei Avadanei, Chief Executive Officer	SC BIT SENTINEL SECURITY SRL
Email: andrei@bit-sentinel.com	RO34300479 / J07/123/2015
Phone: +40 746 649 998	Strada Maria Rosetti 6, Rosetti Tower, Bucharest, Romania

1. Document Information

This document contains a description of Bit Sentinel Security CERT as part of BIT SENTINEL SECURITY SRL, hereinafter referred to as the BSS-CERT, in accordance to RFC 2350 "Expectations for Computer Security Incident Response", providing basic information about the BSS-CERT team, its channels of communication, its roles, and responsibilities.

1.1 Date of Last Update

This is version 1.0, published in March 2021.

1.2 Distribution List for Notifications

Notifications of updates are submitted to our mailing list when appropriate.

1.3 Locations where this Document May Be Found

The latest available version of the "RFC 2350 Description for BSS-CERT" document is always available at the following URL address:

URL: https://bit-sentinel.com/rfc2350.pdf
Version: 1.0

All other versions of this document are available at the same URL address or by direct contact with the BSS-CERT team.

1.4 Authenticating this Document

This document has been signed with the BSS-CERT's PGP key. The signatures and SHA256 file hashes are also on our website, at:

- https://bit-sentinel.com/rfc2350.pdf.sig

2. Contact Information

2.1 Name of the Team

Bit Sentinel Security CERT
Short name: BSS-CERT

2.2 Address

BIT SENTINEL SECURITY SRL
Str. Maria Rosetti no. 6,
Rosetti Tower Building, 7th floor 020485,
Bucharest, Romania

2.3 Time Zone

EET - Eastern European Time (UTC/GMT + 2 hours)

2.4 Telephone Number

+40 746 649998

2.5 Facsimile Number

For the moment, there is no facsimile number available.

2.6 Other Telecommunication

For the moment, there is no other telecommunication channel available.

2.7 Electronic Mail Address

Incident Reports: security@bit-sentinel.com
Office: contact@bit-sentinel.com

2.8 Public Keys and Encryption Information

The BSS-CERT has a PGP key, whose details are:

User ID: Security <security@bit-sentinel.com>
Fingerprint: 1F92 050F 5A32 5287 924A 79A5 AE0F 52B6 740F EF94
Key type: RSA/4096
Expires: never

The key and its signatures can be found at the usual large public key-servers.

2.9 Team Members

Name	Email	PGP Fingerprint
Andrei Avadanei	andrei@bit-sentinel.com	696E 4EEF E718 7909 39E9 3651 9785 65BA D500 2E92
Lucian Ioan Nitescu	lucian@bit-sentinel.com	8BC1 0A9D 7F0E 0E4C E256 B65D 2C46 257B 2A8D 6C1E

2.10 Other Information

General information about the BSS-CERT, as well as links to various recommended security resources, can be found at https://bit-sentinel.com/

2.11 Points of Customer Contact

The preferred method for contacting the BSS-CERT is via e-mail at security@bit-sentinel.com; All e-mails sent to this address will "biff" the responsible human, or be automatically forwarded to the appropriate backup person, immediately. If you require urgent assistance, put "Urgent" in your email subject line.

If it is not possible (or not advisable for security reasons) to use e-mail, the BSS-CERT can be reached by telephone during regular office hours.

The BSS-CERT's hours of operation are generally restricted to regular business hours (07:00-20:00 Monday to Friday except for holidays).

3. Charter

3.1 Mission Statement

BIT SENTINEL SECURITY SRL is one of the leading companies in Romania and CEE to provide Managed Detect and Respond services (BSS-CERT), Offensive Security, Compliance, Incident Response and Hacking Simulation Services.

With an acknowledged mission to protect businesses against cyber threats, Bit Sentinel Security SRL is a one-stop shop for cybersecurity services being able to work with cutting-edge technologies in Cloud, Web Applications & Services, Mobile and IoT.

From penetration testing to incident response, our team of specialists support organizations to get a handle on a wide range of compliance and risk management initiatives. We provide independent, tailored advice and services that cover all aspects of cybersecurity.

The BIT SENTINEL's next-gen Security Operation Center (BSS-CERT) is a solution designed, operated and managed by experienced and certified security specialists providing offensive and defensive capabilities through the detection, analysis and remediation of cyber threats.

Since it was founded, BIT SENTINEL has focused on providing premium and high quality offensive security services such as advanced black box and white box penetration testing, application code review, forensics and incident response.

BSS-CERT is one of the very first professional SOC-as-a-Service available for customers across all major verticals and industries who need comprehensive detection, response, and threat intelligence capabilities. The SOC is supported by a 24/7 incident response team which is backed by a team of threat hunting, offensive security specialists and a team of risk management and compliance, making BIT SENTINEL a one-stop for the entire cyber security needs of any company.

3.2 Constituency

The BSS-CERT's constituency is composed of all users, systems, and networks from the BIT SENTINEL SECURITY SRL environment and its monitored systems.

BSS-CERT provides its services to industrial facility owners and operators, OT integrators, industrial sector regulators, IT/OT cyber security providers, and research teams. Pro-active security reports, such as emerging threat alerts, threat landscape analysis reports, and security advisories as well as materials containing generic analytics are publicly provided for the wider audience.

3.3 Sponsorship and/or Affiliation

BSS-CERT is a service within the BIT SENTINEL SECURITY SRL company for incident response, research, development, and expertise in the field of cyber-security for BIT SENTINEL SECURITY SRL infrastructure and other partners and Clients infrastructure.

3.4 Authority

The BSS-CERT operates under the auspices of, and with authority delegated by BIT SENTINEL SECURITY SRL responsible defined personnel. All members of the BSS-CERT team are employees or partners of the BIT SENTINEL SECURITY SRL and have all of the powers and responsibilities assigned by the Company Administration and responsible team leaders. All member's actions and responses towards cyber-security incidents and threat intelligence research are performed within the current law background and with the approval of the BIT SENTINEL SECURITY SRL Administration and responsible team leaders in order to fulfill the needs and requirements of the in-scope Clients.

4. Policies

4.1 Types of Incidents and Level of Support

The BSS-CERT is authorized to address all types of computer security incidents and events that occur, or threaten to occur, for all its defined Company and Clients assessed and monitored infrastructures, assets, and applications.

The level of support given by BSS-CERT will vary depending on the type and severity of the incident or issue, the type of constituent, the size of the user community affected, and the BSS-CERT's resources at the time, though in all cases, some response will be made within one working day.

Incidents will be prioritized and resources will be assigned according to their apparent severity and extent.

A limited direct support will be given to end-users, depending on the situation, but they are expected to contact their system administrator, network administrator, or department head for assistance.

The BSS-CERT is committed to keeping the client's administrators and responsible personnel informed of potential vulnerabilities, and where possible, will inform this community of such vulnerabilities before they are actively exploited, following the internal procedure and policies of disclosing such information.

4.2 Co-operation, Interaction and Disclosure of Information

While there are legal, ethical, and contractual restrictions on the flow of information from BSS-CERT, many of which are also outlined within contractual agreements and within the current legislation and all of which will be respected, the BSS-CERT acknowledges its responsibility to and declares its intention to contribute to, the public knowledge of threats vectors and/or Indicators of Compromises (IOC). Therefore, while appropriate measures will be taken to protect the identity and data confidentiality of Clients and employees of our constituency where necessary, the BSS-CERT will otherwise share information freely when this will assist others in resolving or preventing security incidents. They may or may not have legal rights to confidentiality; such rights will of course be respected where they exist.

- Private user information is information about particular users, or in some cases, particular applications, which must be considered confidential for legal, contractual, and/or ethical reasons.

Private user information will not be released in identifiable form outside the BSS-CERT, except as provided for below. If the identity of the user is disguised, then the information can be released freely (for example to show a sample .cshrc file as modified by an intruder, or to demonstrate a particular social engineering attack).

- Intruder information is similar to private user information, but concerns intruders.

While intruder information, and in particular identifying information, will not be released to the public (unless it becomes a matter of public record, for example because criminal charges have been laid), it will be exchanged freely with system administrators and CSIRTs tracking an incident.

- Private site information is technical information about particular systems or sites.

It will not be released without the permission of the site in question, except as provided for below.

- Vulnerability information is technical information about vulnerabilities or attacks, including fixes and workarounds.

Vulnerability information will be released freely, though every effort will be made to inform the relevant vendor before the general public is informed.

- Embarrassing information includes the statement that an incident has occurred, and information about its extent or severity. Embarrassing information may concern a site or a particular user or group of users.

Embarrassing information will not be released without the permission of the site or users in question, except as provided for below.

- Statistical information is embarrassing information with the identifying information stripped off.

Statistical information will be released at the discretion of the BSS-CERT's decision.

- Contact information explains how to reach system administrators and CSIRTs.

Contact information will be released freely, except where the contact person or entity has requested that this not be the case, or where BSS-CERT has reason to believe that the dissemination of this information would not be appreciated.

Potential recipients of information from the BSS-CERT will be classified as follows:

- Because of the nature of their responsibilities and consequent expectations of confidentiality, members of BIT SENTINEL SECURITY SRL management and Clients of BIT SENTINEL SECURITY SRL, along responsible employees from BSS-CERT team, are entitled to receive whatever information is necessary to facilitate the handling of computer security incidents which occur in their jurisdictions.

- The BIT SENTINEL SECURITY SRL employees (outside of BSS-CERT team) will receive no restricted information, except where the affected parties have given permission for the information to be disseminated. Statistical information may be made available to the general BIT SENTINEL SECURITY SRL employees. There is no obligation on the part of the BSS-CERT to report incidents to the community, though it may choose to do so; in particular, it is likely that the BSS-CERT will inform all affected parties of the ways in which they were affected, or will encourage the affected site to do so.

- The public at large will receive no restricted information. In fact, no particular effort will be made to communicate with the public at large, though the BSS-CERT recognizes that, for all intents and purposes, information made available to the community is in effect made available to the community at large, and will tailor the information in consequence.

- The computer security community will be treated the same way the general public is treated. While members of BSS-CERT may participate in discussions within the computer security community, such as newsgroups, mailing lists, and conferences, they will treat such forums as though they were the public at large. While technical issues (including vulnerabilities) may be discussed to any level of detail, any examples taken from BSS-CERT experience will be disguised to avoid identifying the affected parties.

- The press will also be considered as part of the general public. The BSS-CERT will not interact directly with the Press concerning computer security incidents, except to point them toward information already released to the general public. If necessary, information will be provided to the BIT SENTINEL SECURITY SRL management. All incident-related queries will be referred to BIT SENTINEL SECURITY SRL management and responsible BSS-CERT team managers. The above does not affect the ability of members of BSS-CERT to grant interviews on general computer security topics; in fact, they are encouraged to do so, as a public service to the community.

- Other sites and CSIRTs, when they are partners in the investigation of a computer security incident, will in some cases be trusted with the approval of BIT SENTINEL SECURITY SRL management with confidential information. This will happen only if the foreign site's bona fide can be verified, and the information transmitted will be limited to that which is likely to be helpful in resolving the incident. Such information sharing is most likely to happen in the case of sites well known to BSS-CERT. For the purposes of resolving a security incident, otherwise semi-private but relatively harmless user information such as the provenance of connections to user accounts will not be considered highly sensitive, and can be transmitted to a foreign site without excessive precautions. "Intruder information" will be transmitted freely to other system administrators and CSIRTs. "Embarrassing information" can be transmitted when there is reasonable assurance that it will remain confidential, and when it is necessary to resolve an incident.

- Vendors will be considered as foreign CSIRTs for most intents and purposes. The BSS-CERT wishes to encourage vendors of all kinds of networking and computer equipment, software, and services to improve the security of their products. In aid of this, a vulnerability discovered in such a product will be reported to its vendor, along with all technical details needed to identify and fix the problem. Identifying details will not be given to the vendor without the permission of the affected parties.

- Law enforcement officers will receive full cooperation from the BSS-CERT, including any information they require to pursue an investigation, in accordance with the BIT SENTINEL SECURITY SRL internal policies, local rules and regulations and agreements signed with Clients.

4.3 Communication and Authentication

Given the types of information that the BSS-CERT will likely be dealing with, telephones will not be considered sufficiently secure to be used even unencrypted. Unencrypted email will not be considered particularly secure, but will be sufficient for the transmission of low-sensitivity data. If it is necessary to send highly sensitive data by email, PGP or one-time-use symmetric keys will be used. Network file transfers will be considered to be similar to e-mail for these purposes: sensitive data should be encrypted for transmission. All encryptions keys should be transmitted over a separate communication channel (one-time readable password, Signal, Telegram messages, etc.).

Where it is necessary to establish trust, for example before relying on information given to the BSS-CERT, or before disclosing confidential information, the identity and bona fide of the other party will be ascertained to a reasonable degree of trust. Within BIT SENTINEL SECURITY SRL, and with known neighbor sites, referrals from known trusted people will suffice to identify someone. Otherwise, appropriate methods will be used, such as a search of FIRST members and/or TF-CSIRT Trusted Introducer, the use of WHOIS and other Internet registration information, etc, along with telephone call-back or e-mail mail-back to ensure that the party is not an impostor. Incoming e-mail whose data must be trusted will be checked with the originator personally, or by means of digital signatures (PGP, in particular, is supported).

5. Services

5.1 Incident Response

BSS-CERT will assist system administrators 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

- Investigating whether indeed an incident occured.
- Determining the extent of the incident.

5.1.2. Incident Coordination

- Determining the initial cause of the incident (vulnerability exploited).
- Facilitating contact with other sites which may be involved.
- Facilitating contact with Clients Security or Administrator teams and/or appropriate law enforcement officials, if necessary.
- Making reports to other CSIRTs.
- Composing announcements to users, if applicable.

5.1.3. Incident Resolution

- Removing the vulnerability, if applicable.
- Securing the system from the effects of the incident.
- Evaluating whether certain actions are likely to reap results in proportion to their cost and risk, in particular those actions aimed at an eventual prosecution or disciplinary action: collection of evidence after the fact, observation of an incident in progress, setting traps for intruders, etc.
- Collecting evidence where criminal prosecution, or Client disciplinary action, is contemplated.

In addition, BSS-CERT will collect statistics concerning incidents which occur within or involve the BSS-CERT clients, and will notify the community as necessary to assist it in protecting against known attacks.

To make use of BSS-CERT's incident response services, please send e-mail as per section 2.11 above. Please remember that the amount of assistance available will vary according to the parameters described in section 4.1.

5.2 Proactive Activities

The BSS-CERT coordinates and maintains the following services to the extent possible depending on its resources:

- Information services
  - List of departmental security contacts, administrative and technical. These lists will be available to the general public, via commonly-available channels such as the World Wide Web and/or the Domain Name Service.
  - Mailing lists to inform security contacts of new information relevant to their computing environments. These lists will be available only to Clients system administrators.
  - Repository of vendor-provided and other security-related patches for various operating systems. This repository will be available to the general public wherever license restrictions allow it, and will be provided via commonly-available channels such as the World Wide Web and/or sftp.
  - Repository of security tools and documentation for use by sysadmins. Where possible, precompiled ready-to-install versions will be supplied. These will be supplied to the general public via www or sftp as above.
  - "Clipping" service for various existing resources, such as major mailing lists and newsgroups. The resulting clippings will be made available either on the restricted mailing list or on the web site, depending on their sensitivity and urgency.
- Training services
  - Members of the BSS-CERT will give periodic seminars on computer security related topics; these seminars will be created for Clients system administrators, developers etc.
- Auditing services
- Archiving services
- Research & Development
  - Research and development of new techniques, tools and technologies to better monitor, detect and react to threats and security incidents

Detailed descriptions of the above services, along with instructions for joining mailing lists, downloading information, or participating in certain services such as the central logging and file integrity checking services, are available on the BSS-CERT web site, as per section 2.10 above.

6. Incident Reporting Forms

There are no local forms developed yet for reporting incidents to BSS-CERT. Incident reports can be sent to security@bit-sentinel.com. We highly recommend the use of the PGP key found at section "2.8 Public Keys and Encryption Information” to encrypt any private or confidential information. Please make sure that your incident report contains:

- Your contact and organizational information - name and organization name, email, telephone number; and case type;
- IP Addresses and/or Indicators of Compromises (IOC);
- At least an excerpt from a log showing the incident activity;
- Any other information that could assist the BSS-CERT team in understanding the incident case type (files, printscreens, emails, etc.).

7. Disclaimers

While every precaution will be taken in the preparation of information, notifications and alerts, BSS-CERT assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.