RFC 2350

CSIRT-OVH

OVH SAS
OVH SAS

1. Diffusion

TLP :WHITE

Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.

TLP:WHITE information may be distributed without restriction, subject to copyright controls.

2. Document Information

This document contains a description of CSIRT-OVH as implemented by RFC 2350[1] . It provides basic information about CSIRT-OVH, its channels of communication, its roles and responsibilities.

2.1. Revisions

Date	Version	Author	Comment
28/12/2018	0.0	SMT	Initialization
17/01/2019	0.1	SMT	Fill the blanks
22/01/2019	0.2	SMT	Clarifications about OVH US LLC
25/01/2019	0.3	SMT	Privacy mentioned as a type of incident.
30/01/2019	1.0	SMT	Last review + Phone number

2.2. Distribution List for Notifications

There is no distribution list for notifications.

2.3. Locations where the Document May Be Found

The current and latest version of this document is available from CSIRT-OVH's website at the following location:

https://csirt.ovh.com/CSIRT_OVH_RFC2350.pdf

2.4. Authenticating this Document

This document has been signed with the PGP key of CSIRT-OVH. The signature is available from CSIRT-OVH's website at the following location:

https://csirt.ovh.com/CSIRT_OVH_RFC2350.pdf.sig

2.5. Document Identification

Title : CSIRT-OVH – RFC 2350
Version : 1.0
Document Date : 2019-01-17
Expiration : this document is valid until superseded by a later version.

[1] http://www.ietf.org/rfc/rfc2350.txt

3. Contact Information

3.1. Name of the Team

CSIRT-OVH

3.2. Address

OVH SAS
SU.Security - CSIRT-OVH
2 Rue Kellerman
BP 80157
59100 Roubaix
France

3.3. Timezone

CET/CEST

3.4. Telephone Number

+33 9 72 61 30 01

3.5. Facsimile Number

Not available.

3.6. Electronic Mail Address

csirt@ovh.com

3.7. Other Telecommunication

Not available.

3.8. Public Keys and Encryption Information

CSIRT-OVH uses the following PGP Key :

- ID : 0x43F7C95E4EB57EF1
- Fingerprint : 14C8 23DD F9A6 F985 78A3 1DD2 43F7 C95E 4EB5 7EF1

The key can be retrieved at any time from applicable public key servers such as https://pgp.circl.lu/. The key shall be used whenever information must be sent to CSIRT-OVH in a secure manner.

3.9. Team Members

CSIRT-OVH's team leader is Sébastien Mériot.

The team consists of IT Security Analysts.

3.10. Other Information

General information about CSIRT-OVH can be found at the following URL:

https://csirt.ovh.com/

3.11. Points of Contact

The preferred method to contact CSIRT-OVH is by sending an email to the following address: csirt@ovh.com.

A security analyst can be contacted at this email address during hours of operation.

Urgent cases can be reported by phone (+33 9 72 61 30 01) during French business hours.

CSIRT-OVH's hours of operation are usually restricted to regular French business hours (Monday to Friday 10:00 to 18:30).

4. Charter

4.1. Mission Statement

Within OVH Group, the Security Unit (or SUS) translates the security strategy in actionable plans, oversees the level of implemented security controls, responds to incidents and establishes operational security baseline.

CSIRT-OVH is the Group's squad in charge of digital forensics and incident responses (DFIR), malware analysis and threat intelligence activities.

CSIRT-OVH's main mission is to support OVH Group's reliability and to protect the company from the threats that would hamper the integrity of its informational and infrastructural assets or damage its reputation. CSIRT-OVH's activities cover prevention, detection, response and recovery.

4.2. Constituency

The constituency of CSIRT-OVH is composed of all the elements of the Information Systems of OVH EMEA (France, Germany, Italy, Morocco, Poland, Portugal, Spain, Tunisia, the UK and any future subsiriary or datacenter to be opened in the Europe area) , OVH Canada and OVH APAC (Australia, India and Singapore) which includes:

- the users;
- the infrastructures;
- the applications;
- the networks and the backbone.

The Information System of OVH US LLC is not part of CSIRT-OVH's constituency.

4.3. Affiliation

CSIRT-OVH is affiliated to OVH Group. It maintains contacts with various national and international CSIRT and CERT teams as well as security teams all around the World whenever such communication follows OVH Group's needs and communication culture.

4.4. Authority

CSIRT-OVH operates under the authority of OVH Group Chief Information Officer.

5. Policies

5.1. Types of Incidents and Level of Support

CSIRT-OVH handles all types of incidents impacting the confidentiality, integrity, availability, traceability or privacy of OVH Group's IT assets.

Depending on the security incident, CSIRT-OVH's expertise may cover - but is not limited to the areas of incident response – digital forensics, malware analysis, strategical, tactical and operational threat intelligence.

The level of support given by CSIRT-OVH will vary depending on the severity of the security incident or issue, its potential or assessed impact and the available CSIRT-OVH's resources at the time of the incident.

5.2. Co-operation, Interaction and Disclosure of Information

CISRT-OVH highly considers the importance of operational coordination and information sharing between CERTs, CSIRTs, SOCs and similar internal and external bodies, since such cooperative actions are likely to improve CSIRT-OVH's efficiency at solving day-to-day problems and specific incidents. The same goes for external information sharing when CSIRT-OVH's cooperation is likely to enable third-party CERTs, CSIRTS and other security teams to better perform their duties and resolve incidents.

CSIRT-OVH operates within the current French legal framework.

5.3. Communication and Authentication

CSIRT-OVH protects sensitive information in accordance with relevant French, European and OVH Group's regulations and policies for applicable jurisdictions. In particular, CSIRT-OVH respects the sensitivity markings allocated by originators of information communicated to CSIRT-OVH ("originator control").

CSIRT-OVH also recognizes and follows the FIRST TLP (Information Sharing Traffic Light Protocol) version 1.0[2].

Communication security, including both encryption and authentication, is achieved by using PGP or any other agreed and tested means, depending on sensitivity and context.

[2] https://www.trusted-introducer.org/ISTLP.pdf

6. Services

6.1. Announcements

CSIRT-OVH provides announcements in the form of alerts and security bulletin featuring threat intelligence of different sorts in order to highlight new threats and the related security measures needed to protect its constituency's Information Systems.

6.2. Alerts and Warnings

CSIRT-OVH disseminates information and intelligence on cyberattacks, technical disruptions, security vulnerabilities, intrusion alerts, malware, and provides recommendations on how to tackle the issue within its constituency. Alerts and warnings may be passed on to other CERTs, CSIRTs, SOCs and security teams if deemed necessary or useful to them on a need-to-know basis.

6.3. Education and Training

CSIRT-OVH provides trainings and security awareness to its constituency to ensure the whys and wherefores of the information security is clearly understood. Training sessions are also scheduled to provide technical experts good practices while responding a security incident.

6.4. Development of Security Tools

CSIRT-OVH develops security tools for its own use, to improve its services and support its activities as needed. These security tools can be used by other members of its constituency or by members of the larger CERT, CSIRT, SOC and broader information security community.

6.5. Intrusion Detection

CSIRT-OVH leverages a number of systems and processes to detect potential intrusions.

6.6. Digital Forensics and Incident Response (DFIR)

CSIRT-OVH performs digital forensics activities whenever necessary, including but not limited to log analysis, memory forensics, physical/virtual drive forensics and network forensics along with the malware analysis activities, which may result from identified forensic needs.

CSIRT-OVH performs incident response for its constituency. The incident response service as developed by CSIRT-OVH covers the 6 phases of the Incident Response process:

- Preparation,
- Identification
- Containment
- Eradication
- Recovery
- Lessons to be learned

7. Incident Reporting Forms

No local form has been developed to report incidents to CSIRT-OVH.

To report an external incident from the outside, please provide the following details to CSIRT-OVH:

- Contact details and organizational information, such as person or organization's name, address and contact information;
- Email address, phone number, PGP key if available;
- IP address(es), FQDN(s), and any other relevant technical element or comment;
- Supporting technical elements such as logs, proof of concept, screenshots, or any other artefact that help our analysts processing your report.

Should you desire to forward any email message to CSIRT-OVH, please include all relevant email headers, bodies and attachments if possible and as allowed by the regulations, policies and legislation under which you operate.

8. Disclaimers

CSIRT-OVH is going to take every precaution in the preparation of information, notifications and alerts. Nevertheless, CSIRT-OVH assumes no responsibility for errors or omissions, or for damages resulting from the use of the information it provides.