CSIRT DESCRIPTION FOR CERT-XLM RFC2350

CERT-XLM

Reference	CERT-XLM-RFC2350.DOCX
Originator	CERT-XLM
Audience	EXCELLIUM|EXTERNAL
Sharing level	TLP:WHITE
Classification	PUBLIC

Document Versioning

Approval

	Name	Date
Prepared By:	Paul Jung	02/11/2016
Verified By:		
Approved By:	Christophe Bianco	03/11/2016

History

Version	Date	Author	Description
1.3	02/11/2016	Paul Jung	User modifications, working time, location, emails.
1.2	25/03/2016	Paul Jung	User addition
1.1	03/04/2015	Paul Jung	User addition – Address changes
1.0	27/01/2015	Paul Jung	Initial version.

Distribution List

Version	Company	Name
1.3	N/A	Public document

About this document.

Date of Last Update

This is the v1.3 version released on 02 November 2016.

Distribution List for Notifications

Distribution List for Notifications changes to this document are not distributed by a mailing-list, RSS or any other mechanism. Please address any specific questions or remarks to CERT-XLM e-mail address (see chapter Electronic Mail Address)

Locations where this Document May Be Found

The current version of this CSIRT description document is available in pdf format on the CERT-XLM WWW site. Its URL is;

http://www.excellium-services.com/wp-content/uploads/2016/11/CERT-XLM-RFC2350.pdf

Please make sure you are using the latest version.

Authenticating this Document

These documents have been signed with the CERT-XLM's PGP key. The signatures are available on our Web site, under:

http://www.excellium-services.com/wp-content/uploads/2016/11/CERT-XLM-RFC2350.pdf.asc

Contact Information

Name of the Team

«**CERT-XLM**»: Excellium CSIRT of Excellium Services S.A.

Address

CERT-XLM

Excellium Services S.A.
5 rue de Goell
L-5326 Contern
Luxembourg

Time Zone

CET / CEST

- GMT+01:00 in winter time (from last Sunday in November to last Sunday in March).
- GMT+02:00 during summer time (from last Sunday in April to last Sunday in October).

Telephone Number

- +352 262 039 64 708 Cert-XLM direct number.
- +352 661 348 273 Excellium Services SOC.

Facsimile Number

None available

Other Telecommunication

None available.

Electronic Mail Address

All incident report should be submitted to <**CERT(at)excellium-services.com**>. This is a mail alias that relays mail to the human(s) on duty for the CERT-XLM.

Public Keys and Other Encryption Information

The CERT-XLM has a PGP key, whose KeyID is **0xD74E5AC0** the related fingerprint is **8D78D1A67F2BAFDE41B74DBA67B311E5D74E5AC0**.

The public key and its signatures can be found at the usual large public key servers, or on CERT-XLM web site, under: http://www.excellium-services.com/wp-content/uploads/2015/01/CERT-XLM_PKEY.asc

Each CERT-XLM team member has also a respective OpenPGP public key that you can fetch from the Excellium Services website.

Team Members

CERT coordination will be performed by Paul Jung. All team members, along with their areas of expertise and contact information, are listed below;

Core Team

Name	**Email**	**KeyID**	**Role**
Paul Jung	pjung(at)excellium-services.com	0x2BD01DE5	Coordinator
	Fingerprint	B851F185CBE40165388E840FFDC487D42BD01DE5	
Yoann Chevalier	ychevalier(at)excellium-services.com	0x43A08EDA	Core team
	Fingerprint	84236875C8CFAA31D2AFBF8FE1E4A65243A08EDA	
Valentin Giannini	vgiannini(at)excellium-services.com	0x0EED79AF	Core team
	Fingerprint	E5BD132628CA96AD7612BF97CFF14A1C0EED79AF	
Vincent Noyalet	vnoyalet(at)excellium-services.com	0xDD951491	Core team
	Fingerprint	0496DFC1F73F7F29A70C42FFA511797EDD951491	

L1 Incident handling may be performed by the following team.

Name	**Email**	**KeyID**	**Role**
Farid Bouraïne	Fbouraine(at)excellium-services.com	0xC9452430	Incident handler
	Fingerprint	071AEC47E518C664C2CCA7A5F0069F6CC9452430	
Sebastien Kaiser	skaiser(at)excellium-services.com	0x7135874A	Incident handler
	Fingerprint	325EC97B5EB358DEABBE143556ADCD9E7135874A	
Christophe Rosenkranz	crosenkranz(at)excellium-services.com	0x2AD5D972	Incident handler
	Fingerprint	E6E258F899C30F04242413E9D8CE98852AD5D972	

Staff augmentation team for specific needs.

Name	Email	KeyID	Role
Remi Sinicco	rsinicco(at)excellium-services.com	0x5E2A4B3B	Incident handler
	Fingerprint	035F4BCD243B01569C4B84F267EBE2A85E2A4B3B	
Loic Hernandez	lhernandez(at)excellium-services.com	0xBE94EEE4	Incident handler
	Fingerprint	4DBC8BD9966B9A7DED4965556B7BD9E8BE94EEE4	
Pierre Ruaro	pruaro(at)excellium-services.com	0xD256F530	Incident handler
	Fingerprint	CC5755DD62AD106CBC1560C22198898AD256F530	
Gordi Comunello	gcomunello(at)excellium-services.com	0xA7630D8D	Incident handler
	Fingerprint	9F0ED3B66DF42F8049A6DE5D1F487E78A7630D8D	
Martin Grandcolas	mgrandcolas(at)excellium-services.com	0xBE752074	Incident handler
	Fingerprint	6B4BBCC6876CDC2DA5C5E56C57934C5BBE752074	
Adrien Jolibert	ajolibert(at)excellium-services.com	0x6B606530	Incident handler
	Fingerprint	A814B4DF9089AD79E546B4B06A9FCF5A6B606530	
Dominique Righetto	drighetto(at)excellium-services.com	0x841850BB	Incident handler
	Fingerprint	291A5A85CC65EACA8747EEAC327DF7CA841850BB	

Business and legal support team members are:

Name	Email	KeyID	Role
Christophe Bianco	cbianco(at)excellium-services.com	0xE684F47E	Business support
	Fingerprint	46554E3FC0D37028FE0965AD8C096982E684F47E	
Xavier Vincens	xvincens(at)excellium-services.com	0x30D41DA1	Business support
	Fingerprint	837F21DAAB6B2A4FC58D7584FD20EBE230D41DA1	

Other Information

General information about the CERT-XLM, as well as links to various recommended security resources, can be found at http://www.excellium-services.com/CERT-XLM

Points of Customer Contact

The preferred method for contacting the CERT-XLM is via e-mail at <**cert(at)excellium-services.com**>; e-mail sent to this address will be automatically forwarded to the on call person If you require urgent assistance, put «**[URGENT]**» in your subject line.

Emails could be encrypted using pgp. CERT-XLM public key information are detailed in the chapter Public Keys and Other Encryption Information.

If it is not possible (or not advisable for security reasons) to use e-mail, the CERT-XLM can be reached by telephone during regular office hours. (See chapter Telephone Number) Outside theses hours, incidents will be registered on 24/7 through his SOC. Use in this case the urgency number referenced in chapter Telephone Number)

If possible, when submitting your report, use the form mentioned in section Incident Reporting Forms.

Charter

Mission statement

The purpose of the CERT-XLM is to assist Excellium customers located in Luxembourg and Belgium by implementing proactive measures to reduce the risks of computer security incidents, and second, assist them in responding when such incidents when they occur. For assuring this mission, CERT-XLM may work in coordination with various CERTs and SOCs.

CERT-XLM will also act as a CSIRT bridge to PSF (*Professionnels du Secteur Financier*) entities in Luxembourg to improve reaction and to coordination in case of incidents.

Additionally, CERT-XLM will release security notices based on relevancy of information.

Constituency

CERT-XLM is the Computer Security Incident Response Team of Excellium Services S.A.

The constituency will cover various TLD, Internet Public ASN and IP addresses located/originated and/or operating in/from his customers.

Sponsorship and/or affiliation

CERT-XLM is a private CSIRT. It is owned, and operated by Excellium services.

It maintains relationships with various CSIRTs in Luxembourg and Belgium

CERT-XLM is listed as team member of CERT.lu since

https://www.cert.lu/#members

CERT-XLM is officially listed as accredited team since 23 January 2015.

http://www.trusted-introducer.org/directory/teams/cert-xlm.html

Policies

Types of Incidents and Level of Support

CERT-XLM addresses all types of computer security incidents which occur, or threaten to occur, in the constituency networks. The level of support given by CERT-XLM will vary depending on the type and severity of the incident or issue and CERT's available resources. However, in all cases, some responses will be made.

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

Note that no direct support will be given to end users; they are expected to contact their system administrator, network administrator, or department head for assistance. The CERT-XLM will support the latter people.

Co-operation, Interaction and Disclosure of Information

CERT-XLM will exchanges all necessary information with other CSIRTs as well as with affected parties' administrators.

CERT-XLM will protect sensitive information in accordance with relevant regulations and policies, in particular regarding the rules requested by the CSSF (Commission de Surveillance du Secteur Financier) and the constraints of a support PSF entity.

CERT-XLM will appends Light Traffic Protocol when sharing information with teams that support it and will honors such protocol if present.

Communication and Authentication

In view of the types of information that CERT-XLM deals with, telephones will be considered sufficiently secure to be used even unencrypted.

Unencrypted e-mail 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 (i.e. information classified as Confidential) by e-mail, encryption (preferably PGP) will be used.

All e-mail or data communication originating from CERT-XLM will be digitally signed, using the generic PGP key mentioned above or the CERT team members own signature keys.

Services

Incident Response

CERT-XLM will assist system owner in handling the technical and organizational aspects of incidents. In particular, it will provide assistance or advice with respect to the following aspects of incidents management.

Incident Triage

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

Incident Coordination

- Determining the initial cause of the incident.
- Facilitating contact with other sites which may be involved.
- Facilitating contact with the constituency and/or appropriate law enforcement officials, if necessary.
- Making reports to other CSIRTs.
- Composing announcements to users, if applicable .

Incident Resolution

Note: This set of service includes also incident response on-site.

- Removing the vulnerability.
- 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 University disciplinary action, is contemplated.

In addition, CERT-XLM will collect statistics concerning incidents and threats which occur within his customers and will notify the community as necessary to assist it in protecting against known attacks.

For requesting CERT-XLM services please refer to section «Incident Reporting Forms» and «Contact Information» for points of contact.

Please remember that amount of assistance will vary as described in section «Mission statement».

Proactive Activities

Regarding his resources CERT-XLM will coordinates and maintains the following services:

- List of vulnerabilities.
- Threat notification.
- Training and educational services.
- Technical analysis.

Incident Reporting Forms

CERT-XLM strongly encourages anyone reporting an incident to fill it out the reporting form. The current version of the form is available from http://www.excellium-services.com/wp-content/uploads/2015/01/CERT-XLM-Incident-Reporting-Form.pdf

Disclaimers

While every precaution will be taken in the preparation of information, notifications and alerts, CERT-XLM assumes no responsibility for errors or omissions, or for damages.

[End of document]