TLP:WHITE

RFC 2350 CERT Pirelli Description Document

TLP:WHITE

1. DOCUMENT INFORMATION

This document contains a description of CERT Pirelli in accordance with RFC 2350[1]. It provides basic information about its contact information, structure, policies, and provided services. CERT Pirelli is a Computer Security Incident Response Team (CSIRT) established within the Pirelli Security Office authority.

1.1. Date of last update

Version 1.0, published the 08/07/2019.

1.2. Distribution List for Notifications

CERT Pirelli will not define a distribution List for Notification.

1.3. Locations where this Document May Be Found

An up to date version of this document can be found at: https://corporate.pirelli.com/corporate/en-ww/aboutus/pirelli-cert.

1.4. Authenticating this Document

This document has been signed with the PGP key of CERT Pirelli.

See section 2.8 for more details.

2. CONTACT INFORMATION

2.1. Name of the Team

Team Name: CERT Pirelli

Short Team Name: CERT-P

2.2. Address

Pirelli & C S.p.A.

Viale Piero e Alberto Pirelli n. 25

20126 Milan (MI), Italy

2.3. Time Zone

CET – Central European Time (GMT+0100), CEST – Central European Summertime (GMT+0200).

[1] This document's template is based on Request for Comments (RFC) 2350, "*Expectations for Computer Security Incident Response - Appendix D: Outline for CSIRT template*".

2.4. Telephone Number

+39 02 6442 51741

2.5. Fax Number

N/A

2.6. Other Telecommunication

N/A

2.7. Electronic Mail Address

cert@pirelli.com

2.8. Public Keys and Encryption Information

CERT Pirelli is supporting secure communication through the following PGP Key:

- Key-ID: 0xFF9D038E
- User-ID: Pirelli CERT <cert@pirelli.com>
- Fingerprint: D35E B24D 1A30 0984 910D 2522 4C75 91BC FF9D 038E

Additionally, the key can be found at: https://www.pirelli.com/.well-known/cert-pirelli-key.txt, and on PGP Server: http://pgp.mit.edu.

2.9. Team Members

The Head of CERT Pirelli is Andrea Modesto Rossi. The operational CERT Team is comprised of mixture of technical and governance analysts, which are committed in delivering high quality CERT services to their constituency.

2.10. Other Information

N/A

2.11. Points of Customer Contact

CERT Pirelli's preferred method of contact is email.

Contact can be made by sending an email to: cert@pirelli.com (This mailbox is monitored during operation hours: (Mon-Fri 09:00-18:00). Please be aware that CERT Pirelli will accept only PGP signed emails.

For those who are adopting the Traffic Light Protocol (TLP) v1.0, please indicate the TLP color in the email's Subject and body. The TLP color must be in capital letters, as per example below:

TLP:RED, TLP:AMBER, TLP:GREEN, or TLP:WHITE.

In addition to the above, urgent matters can be reported by calling: +39 026442 51741.

3. CHARTER

3.1. Mission Statement

CERT Pirelli's mission is to improve the overall information resilience and cyber security posture of the Pirelli Group, through a proactive security incident response and risk management approach.

3.2. Constituency

CERT Pirelli's serves a constituency of technical and non-technical users within the entire Pirelli group network infrastructure.

3.3. Sponsorship and/or Affiliation

Not disclosed.

3.4. Authority

CERT Pirelli services are operating in compliance with Pirelli's security governance framework and is also under the authority of Pirelli's Chief Information Security Officer.

4. POLICIES

4.1. Types of Incidents and Level of Support

CERT Pirelli is authorized to manage all information security incidents that occurs within Pirelli group's network infrastructure.

The team is serving its constituency with reactive, proactive and security quality management services.

4.2. Co-operation, Interaction and Disclosure of Information

CERT Pirelli is committed to co-operate, interact and disclose information with Italian, European and International CSIRT/CERT community.

The team is proactively committed in cultural exchange within the CERT community. For this reason, all worldwide CERT teams are welcome to get in touch with CERT Pirelli to establish co-operation agreements, interactions or information sharing initiatives.

4.3. Communication and Authentication

CERT Pirelli is committed to guarantee and establish secure communication at all times.

5. SERVICES

CERT Pirelli is providing:

- Reactive Services
- Proactive Services
- Security Quality management Services

5.1. Reactive services

Reactive services are designed to respond to requests for assistance, reports of incidents from Pirelli Group constituency, and any threat or attack against the Pirelli group. In particular, the team is committed to deliver alerts and warnings, incident handling, vulnerability handling and artifact handling services for its constituency. Alerts and warnings will also be provided externally when required.

5.2. Proactive activities

The Proactive services are designed to improve Pirelli's Group network infrastructure resilience and security processes, before any incident or event occurs or is detected. The main goal is to avoid incidents and to reduce their impact and scope when they do occur.

5.3. Security quality management services

CERT Pirelli serves its constituency with security quality management services, such as risk analysis, security consulting, awareness building and education and training. Services that fall into this category are not unique to incident handling or CERT Pirelli's services. They are well-known, established services designed to improve Pirelli Group's resilience and cybersecurity posture. By leveraging the experiences gained in providing the reactive and proactive services described above, a CERT Pirelli will bring unique input to these quality management services. These services are designed to incorporate feedback and lessons learned based on knowledge gained by responding to incidents, vulnerabilities, and attacks. Feeding such experiences into the established traditional services as part of a security quality management process will likely improve Pirelli Group long-term security efforts. The CERT Team governance analysts will contribute, as subject matter experts, to Pirelli Security Office risk analysis, Security consulting and awareness building projects.

6. INCIDENT REPORTING FORMS

CERT Pirelli has developed and implemented an internal incident reporting process for its constituency.

All incidents reported from outside Pirelli constituency should be reported at: cert@pirelli.com

Please use the following structure when reporting an incident:

- Reporting person contact details;
- Date and time of the incident;

- Type of incident;
- Reason for reporting;
- Incident's Relevant Technical information.

7. DISCLAIMERS

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