myCloudDoor

RFC 2350
CSIRT for MYCD-CERT
CYBERSEC

DISCOVER CYBERSEC TRANSFORM OPTIMIZE INNOVATE EMPOWER

myCloudDoor.com

1 | ABOUT THIS DOCUMENT

1.1 Date of Last Update

This is version 1.02, published 2024/08/01.

1.2 Distribution List for Notifications

Notifications of updates are submitted to our mailing list.
Subscription and unsubscription requests for this list should be sent to the email address at
<cybersec@mycloudddoor>

1.3 Locations where this Document May Be Found

The current version of this CSIRT description document is available from the MYCD-CERT WWW site; its URL is http://www.mycd-cert.com/MYCD-CERT/CSIRT-descr.txt
Please make sure you are using the latest version.

1.4 Authenticating this Document

This document have been signed with the MYCD-CERT's PGP key.
The signatures are also on our Web site, under:
http://www.mycd-cert.com/MYCD-CERT/CSIRT-descr.asc

2 | CONTACT INFORMATION

2.1 Name of the Team

"MYCD-CERT": Cybersecurity Incident Response Center - myClouDoor.

2.2 Address

MYCD-CERT
MYCLOUDDOOR SECURITY & INNOVATION, S.L.
Avenida Cortes Valencianas, 39, 46015
Valencia
Spain

2.3 Time Zone

CET (UTC+1, and UTC+2 from April to October)

2.4 Telephone Number

+34 910.558.845 (ask for the SOC MYCD-CERT)

2.5 Facsimile Number

None available

2.6 Other Telecommunication

None available.

2.7 Electronic Mail Address

<cybersec@mycloudddoor.com> This is a mail alias that relays mail to the human(s) on duty for the MYCD-CERT.

2.8 Public Keys and Other Encryption Information

The MYCD-CERT has a PGP key and its content is:

-----BEGIN PGP PUBLIC KEY BLOCK-----
Comment: ID de usuario: Cybersec <cybersec@mycloudddoor.com>
Comment: Válido desde: 16/01/2024 13:34
Comment: Válido hasta: 16/01/2027 12:00
Comment: Tipo: 255-bit EdDSA (clave secreta disponible)
Comment: Uso: Firmado, Cifrado, ID de la certificación
Comment: Huella digital: F362A99B55EEFABFB7921B4E69D00571336FE640

mDMEZaZ3zBYJKwYBBAHaRw8BAQdAnWSD8++pZhHiy9hnB/s47a1RmFNb1DOg6hjIXSC
nH+y0I0N5YmVyc2VjIDxjeWJlcnNlY0BteWNsb3VkZG9vci5jb20+iJkEExYKAEEWIQTzYqmb
Ve76v7eSG05p0AVxM2/mQAUCZaZ3zAIbAwUJBaTV5AULCQgHAgIiAgYVCgkICwIEFgIDA
QIeBwIXgAAKCRBp0AVxM2/mQF9/AP9zZWSCrgLZF0NNc+4rfj7GUSoTRVcUz1dXiUPmNT
sK6AD+Ikskh0jutqnYFKMV08keLC+rBEFAZ8KY4FI5M5iUbAa4OARlpnfMEgorBgEEAZdVA
QUBAQdAHADnhYrWzHUd+KUHaAhMrWU9z9LwxihacWAmTujaS0ADAQgHiH4EGBYKAC
YWIQTzYqmbVe76v7eSG05p0AVxM2/mQAUCZaZ3zAIbDAUJBaTV5AAKCRBp0AVxM2/mQ
G7qAP0fBnbr3A6Hps1au1/XSHZ6z8rcLjx4ijUBS98y+PgQOwD/Sjpyx8Z0ly7b4arMDCYua
mQ5duiu5DZd6PkrGY6cDQ0==jYhb
-----END PGP PUBLIC KEY BLOCK-----

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

2.9 Team Members

Miguel Monedero, Head of Information Security at myCloudDoor and MYCD-CERT. Management, liaison and supervision are provided by Miguel Monedero.

Christopher Domingo, Manager of myCloudDoor SOC/Unit and MYCD-CERT

Carlos Jesus Pérez, Manager of myCloudDoor Architecture and MYCD-CERT

Backup coordinators and other team members, along with their contact information, are listed in the MYCD-CERT web pages, at
http://www.mycloudddoor.com/cybersec/teamlist.txt

2.10 Other Information

General information about the MYCD-CERT, as well as links to various recommended security resources, can be found at
https://www.mycloudddoor.com/cybersec/mycd-cert

2.11 Points of Customer Contact

The preferred method for contacting the MYCD-CERT is via e-mail at <cybersec@mycloudddoor.com>; e-mail 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 subject line.

If it is not possible (or not advisable for security reasons) to use e-mail, the MYCD-CERT can be reached by telephone during regular office hours. Telephone messages are checked less often than e-mail.

The MYCD-CERT's hours of operation are generally restricted to regular business hours (09:00-19:00 Monday to Friday except holidays).

If possible, when submitting your report, use the form mentioned in section 6.

3 | CHARTER

3.1 Mission Statement

The purpose of the MYCD-CERT is, first, to assist members of myCloudDoor and its clients in implementing proactive measures to reduce the risks of computer security

incidents, and second, to assist myCloudDoor in responding to such incidents when they occur.

3.2 Constituency

The MYCD-CERT's constituency is the myCloudDoor employees and its clients.

3.3 Sponsorship and/or Affiliation

The MYCD-CERT is sponsored by its constituents.
It maintains affiliations with various CSIRTs throughout Spain on an as needed basis.

3.4 Authority

We coordinate security incidents on behalf of our constituency and at our constituents request.

4 | POLICIES

4.1 Types of Incidents and Level of Support

The MYCD-CERT is authorized to address all types of computer security incidents which occur, or threaten to occur, at myCloudDoor or its clients.

The level of support given by MYCD-CERT will vary depending on the type and severity of the incident or issue, the type of constituent, and the MYCD-CERT's resources at the time, though in all cases some response will be made within one working day.
Resources will be assigned according to the following priorities, listed in decreasing order:

- Threats to the physical safety of human beings.
- Root or system-level attacks on any Management Information System, or any part of the backbone network infrastructure.
- Root or system-level attacks on any large public service machine, either multi-user or dedicated-purpose.
- Compromise of restricted confidential service accounts or software installations, in particular those used for MIS applications containing confidential data, or those used for system administration.
- Denial of service attacks on any of the above three items.
- Any of the above at other sites, originating from XYZ University.

- Large-scale attacks of any kind, e.g. sniffing attacks, IRC "social engineering" attacks, password cracking attacks.
- Threats, harassment, and other criminal offenses involving individual user accounts.
- Compromise of individual user accounts on multi-user systems.
- Compromise of desktop systems.
- Forgery and misrepresentation, and other security-related violations of local rules and regulations, e.g. netnews and e-mail forgery, unauthorized use of IRC bots.
- Denial of service on individual user accounts, e.g. mailbombing.

Types of incidents other than those mentioned above will be prioritized according to their apparent severity and extent.

4.2 Co-operation, Interaction and Disclosure of Information

While there are legal and ethical restrictions on the flow of information from MYCD-CERT, many of which are also outlined in the myCloudDoor Security Policy, and all of which will be respected,
the MYCD-CERT acknowledges its indebtedness to, and declares its intention to contribute to, the spirit of cooperation that created the Internet.
Therefore, while appropriate measures will be taken to protect the identity of members of our constituency and members of neighbouring sites where necessary, the MYCD-CERT will otherwise share information freely when this will assist others in resolving or preventing security incidents.

In the paragraphs below, "affected parties" refers to the legitimate owners, operators, and users of the relevant computing facilities. It does not refer to unauthorized users, including otherwise authorized users making unauthorized use of a facility; such intruders may have no expectation of confidentiality from the MYCD-CERT. They may or may not have legal rights to confidentiality; such rights will of course be respected where they exist.

Information being considered for release will be classified as follows:

- 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 be not be released in identifiable form outside the MYCD-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 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 Computing Services Department.

- 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 MYCD-CERT has reason to believe that the dissemination of this information would not be appreciated.

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

- Because of the nature of their responsibilities and consequent expectations of confidentiality, members of myCloudDoor management are entitled to receive whatever information is necessary to facilitate the handling of computer security incidents which occur in their jurisdictions.

- Users at myCloudDoor are entitled to information which pertains to the security of their own computer accounts, even if this means revealing "intruder information", or "embarrassing information" about another user. For example, if account aaaa is cracked and the intruder attacks account bbbb, user bbbb is entitled to know that aaaa was cracked, and how the attack on the bbbb account was executed. User bbbb is also entitled, if she or he requests it, to information about account aaaa which might enable bbbb to investigate the attack. For example, if bbbb was attacked by someone remotely connected to aaaa, bbbb should be told the provenance of the connections to aaaa, even though this information would ordinarily be considered private to aaaa. Users at myCloudDoor are entitled to be notified if their account is believed to have been compromised.

- The myCloudDoor community 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 myCloudDoor community. There is no obligation on the part of the MYCD-CERT to report incidents to the community, though it may choose to do so; in particular, it is likely that the MYCD-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 MYCD-CERT recognizes that, for all intents and purposes, information made available to the myCloudDoor 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 MYCD-CERT may participate in discussions within the computer security community, such as newsgroups, mailing lists (including the full-disclosure list "bugtraq"), 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 MYCD-CERT experience will be disguised to avoid identifying the affected parties.

- The press will also be considered as part of the general public. The MYCD-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 myCloudDoor Public Relations Department, and to the Customer Relations group of the Consultoria i Servicios de la Informacion Department. All incident-related queries will be referred to these two bodies. The above does not affect the ability of members of MYCD-CERT to grant interviews on general computer security topics; in fact, they are encouraged to do to, 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 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 MYCD-CERT (for example, several other Quebec universities have informal but well-established working relationships with myCloudDoor in such matters).

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 MYCD-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 MYCD-CERT, including any information they require to pursue an investigation, in accordance with the Policy on Computing Facilities.

4.3 Communication and Authentication

In view of the types of information that the MYCD-CERT will likely be dealing 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 by e-mail, PGP 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.

Where it is necessary to establish trust, for example before relying on information given to the MYCD-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 myCloudDoor, 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, 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

MYCD-CERT coordinates all activities related to incident response within its constituency. We provide support, help, and 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.
    - Determine which constituents are affected by the incident.

5.1.2 Incident Coordination

- Investigate the initial cause of the incident.
    - Contact other affected sites, if necessary.
    - Composing announcements to users, if applicable.
    - Notify other CSIRTs, if appropriate.
    - Maintain current database of sites, networks, domains, and security contacts..

5.1.3 Incident Resolution

- 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 is contemplated.

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

To make use of MYCD-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

- Advisory service
- Maintain a database of networks, sites and security contacts
- Mailing lists for security information
- Regular tutorials on security topics
- Network scans
- Early warning system
- Regular talks on security topics

6 | INCIDENT REPORTING FORMS

We do not have an incident reporting form. Please report security incidents via encrypted e-mail to <cybersec@mycloudddoor.com>.

Incident reports should contain the following information:

Incident date and time (including time zone)
Source IPs, ports, and protocols
Destination IPs, ports, and protocols
Preferable the report includes a log file in a common format.

7 | DISCLAIMERS

This document is provided 'as is' without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.

Use of this document is at the user's sole risk. All users expressly agree to this condition of use. If you notice any mistakes within this document please send a message to us by e-mail. We will try to resolve such issues as soon as possible.

myCloudDoor

myCloudDoor.com

GRACIAS

info@mycloudddoor.com

FORT LAUDERDALE (US) · MADRID (SE) · AMSTERDAM (WE) · SANTIAGO DE CHILE (LATAM) · DUBAI (MEA)