

0-Days ACL Analyse **Audit** **Autorité** **Awareness** Botnets **Buffer** **CERT**

Certificats **Code** Conception Cryptographie Cyber-Attacks DCSSI Defacement

Détection Disclosure **DNS** DNSSec **Education** eID ENISA

Firewall **FIRST** Forensic **Guidance** Hacker ICANN Identity IDS IETF

IFRAME Incidents Internet Intrusion IP **IPSec** **IPV6** ISO ISO27001 ISOC IT

LINUX Mail MD5 **Menaces** Méthodologies **MITM** Mobile-Devices NET PDA

Phishing **Planification** Privacy Proxy RBAC **RFC** RFID **Risques** Rootkits

Sécurité Security **Sensibilisation** SHA1 SmartPhones SPAM **SQL** SSH SSL

TCP Technologies Terrorisme Virtualité Virus **VoIP** WEB2 **WEP** Windows WPA

CERT-DEVOTEAM

POLITIQUE DE PUBLICATION D'UNE VULNERABILITE - VULNERABILITY DISCLOSURE POLICY

CONNECTING BUSINESS & TECHNOLOGY

Ce document décrit la politique du CERT-DEVOTEAM pour ce qui concerne la gestion et la publication de vulnérabilités et autres problèmes de sécurité découverts par les équipes du CERT-DEVOTEAM. Il est disponible en Français et Anglais.

This document describes the CERT-DEVOTEAM policy regarding the management and disclosure of security vulnerabilities or other issues discovered by the CERT-DEVOTEAM teams. It is available in both French and English.

POLITIQUE/POLICY

PUBLICATION/DISCLOSURE

Conformément aux bonnes pratiques en la matière, le CERT-DEVOTEAM adopte une politique de publication responsable. Une faille de sécurité ne sera jamais diffusée publiquement, pas plus qu'un code de démonstration ne sera publiquement fourni, sans que toutes les options permettant de corriger cette faille n'aient été explorées et testées. Le CERT-DEVOTEAM s'engage à respecter cette politique

In accordance with the best practices, CERT-DEVOTEAM adopted a responsible disclosure policy. The core principles to be enforced are that neither a security flaw, nor a proof-of-concept will be publicly disclosed or made available, before all the possibilities to solve the flaw are explored and tried. Any CERT-DEVOTEAM member will have to acknowledge and commit to abide by this vulnerability disclosure policy.

Il en ira de même avec toutes les informations concernant un problème de sécurité non encore connu obtenues d'une source tierce.

The same applies for any security issue-related information not yet publically disclosed, and brought to the CERT-DEVOTEAM attention by a third-party.

POINT DE CONTACT/POINT OF CONTACT

Le **CERT-DEVOTEAM** peut être contacté par téléphone ou par messagerie électronique toute la semaine, du Lundi matin au Vendredi soir, de 9h00 à 17h30 heure local Française, hors jours fériés en France.

Nos coordonnées figurent sur notre serveur WEB: <http://www.cert-devoteam.fr/contact.html>

Téléphone : +33 1 69 85 78 90

Mail : info@cert-devoteam.fr

CERT-DEVOTEAM (DEVOTEAM Group CSIRT) <info@cert-devoteam.com>

PGP Fingerprint: 850D 3D63 0BE9 88AB 76DA 50F7 90E4 79BE 1DFF 8EF7

CERT-DEVOTEAM can be reached by phone or electronic mail any working day from Monday mornings to Friday evenings, from 9:00AM to 5:30 PM, French time, except for French public holiday.

Contact details can be found on our WEB server: <http://www.cert-devoteam.com/contact.html>

Phone : +33 169 857 890

Mail : info@cert-devoteam.com

CERT-DEVOTEAM (DEVOTEAM Group CSIRT) <info@cert-devoteam.com>
PGP Fingerprint: 850D 3D63 0BE9 88AB 76DA 50F7 90E4 79BE 1DFF 8EF7

PROCEDURE/PROCESS

La procédure suivante s'applique à tout problème de sécurité non encore connu découvert par nos équipes dans un logiciel, un équipement ou encore un service.

The following process described below is to be enforced for the handling of any yet unknown security issue discovered by our teams in a software application, equipment or service.

1- PREPARATION / PREPARATION

Nous recherchons toutes les informations concernant le service, l'équipe ou la personne la plus à même de traiter notre alerte: noms, numéros de téléphone, adresses de messagerie électronique voire même postale.

We collect all information required to send our advisory to the recipient that may best fits the handling of our warnings, whether a group, a team, or a person in charge of the targeted product, or service, such as name, phone number, electronic or postal mail addresses...

Dans le meilleur des cas, le fournisseur du logiciel, l'opérateur du service, ou le constructeur de l'équipement vulnérable dispose d'un point de contact dédié aux problèmes de sécurité, ou plus souvent au support. Auquel cas, le CERT-DEVOTEAM utilisera les informations fournies pour prendre un premier contact avec eux.

At best, a security contact point dedicated to the handling of security-related issues will be contacted as an entry point. It may also be any support in charge of the vulnerable software, the vulnerable service or the vulnerable equipment. In any case, CERT-DEVOTEAM will use the provided information to establish a first contact.

Dans le pire des cas, quand rien ne peut être trouvé, le CERT-DEVOTEAM obtiendra un identifiant CVE. Le CERT-DEVOTEAM informera ensuite les CSIRTs Français puis le réseau des CSIRTs Européens de la vulnérabilité découverte. Le CERT-DEVOTEAM publiera enfin celle-ci après avoir respecté un délai de précaution de 6 mois (voir Etape 3.2).

At worse, if no details are found, CERT-DEVOTEAM will handle the disclosure, and will first request a CVE identifier. Then, CERT-DEVOTEAM will notify on the discovered vulnerability some or all French CSIRTs and finally, some of the European CSIRTs that are members of the European TF-CSIRT network. CERT-DEVOTEAM will publicly disclose the vulnerability after a 6 month delay (see Step 3.2).

Un premier contact par téléphone ou messagerie électronique permettra d'obtenir si besoin la clef PGP qui sera utilisée pour transmettre notre alerte ou de convenir le cas échéant d'un moyen de transfert sécurisé et non répudiable. L'adresse info@cert-devoteam.com sera utilisée, les courriers seront signés par la clef PGP attachées à cette adresse.

The aim of the first contact by phone or electronic mail be to get the PGP key that will be used to exchange information, such as our alert, or if not available, to define a formal, secure and not deniable communication process. The sender address info@cert-devoteam.com will be used, and all mails will be signed with the appropriate PGP key.

2- NOTIFICATION / NOTIFICATION

Notre alerte sera ensuite transmise sous la forme d'un courrier électronique signé utilisant l'adresse alert@devoteam.com et la clef PGP associée. Ce courrier justifiera l'objet de la notification et contiendra un pointeur sur notre politique de diffusion et sur le processus de publication, à savoir le présent document hébergé sur notre site WEB.

Bonjour,

Notre équipe de sécurité a détecté une vulnérabilité de sécurité (CRITIQUE | IMPORTANTE) dans le produit (NOM DU PRODUIT ou SERVICE) (édité | géré) par (votre société | la société XYZ).

Vous trouverez ci-joint, en attachement, une description de la vulnérabilité CERT-DVT-SECWS-AAAA-NNN ainsi que le détail du processus de publication de l'alerte associée.

Notre politique de diffusion, et le processus de publication associé, sont décrits ici: <http://www.cert-devoteam.fr/contact.html>

N'hésitez pas à nous contacter pour obtenir toutes les informations nécessaires à la reproduction de ce problème et à sa correction. Nous restons à votre disposition pour discuter des modalités de référencement CVE de cette alerte auprès du MITRE, et des étapes de sa publication auprès de la communauté sécurité.

Cordialement,

L'équipe du CERT-DEVOTEAM

Our alert will be sent by the way of a signed mail using the alert@devoteam.com address and the related PGP key. This mail will describe the object of the notification and will give a pointer to our disclosure policy and the related publication process, that is this document hosted on our WEB site.

Hello,

Our security team has detected a (CRITICAL | IMPORTANT) security vulnerability in the (PRODUCT or SERVICE NAME) (developed | managed) by (your company | the XYZ company).

You will find attached a description of the CERT-DVT-SECWS-AAAA-NNN vulnerability along with the detailed disclosure process and planning of the related security advisory.

Our disclosure policy, and the related publication process, are detailed here: <http://www.cert-devoteam.com/contact.html>

Don't hesitate to get in touch with us to obtain all the information required to reproduce and to correct that issue. We will be at your disposal to discuss how to get a CVE number from MITRE for that security alert, and the publication to the security community steps.

Best regards,

The CERT-DEVOTEAM team

La description détaillée du problème de sécurité sera disponible sous la forme d'un document attaché et chiffré avec la clef PGP du destinataire. Ce document sera référencé avec un identifiant de la forme: **CERT-DVT-SECWS-AAAA-NNN** avec AAAA l'année courante, et NNN le numéro d'alerte dans l'année. Ce document respectera un format précis, défini par ailleurs.

A detailed description of the security issue will be made available as an attached text document ciphered with the recipient PGP key. This document will be referenced by an identifier that will follow the following format: **CERT-DVT-SECWS-YYYY-NNN** with YYYY the current year, and NNN the alert number within that year. This document will use a template defined in another guide.

3- ACQUITTEMENT / ACKNOWLEDGMENT

Le traitement de l'alerte transmise doit être confirmé au CERT-DEVOTEAM par l'éditeur, l'opérateur ou le fabricant. Cette confirmation doit intervenir dans les 15 jours ouvrés suivant la réception de notre courrier. Ce délai doit permettre les investigations requises pour déterminer le travail à effectuer et la date prévisionnelle de publication d'un correctif.

Processing of the sent alert should be acknowledged to CERT-DEVOTEAM by the editor, provider or manufacturer. This acknowledgement should be received within the working 15 days after the delivery of our mail. This delay should allow the investigations needed to assess the severity rating of the vulnerability, and in some cases define the amount work to be performed, and forecast a date for a patch be published.

Le problème de sécurité peut avoir déjà fait l'objet d'une notification de la part d'une tierce partie. Auquel cas, l'éditeur, l'opérateur ou le fabricant informera le CERT-DEVOTEAM du délai maximal (Tc) annoncé à ce tiers pour la publication d'une mise à jour ou d'un correctif.

That security issue may have already been notified by a third party. In such a case, the editor, provider or manufacturer will inform CERT-DEVOTEAM of the maximal delay (Tc) announced to this third party for the publication of an update or a patch.

Une relance sera engagée à l'échéance de ce premier délai de 15 jours ouvrables (Etape 2.3). A l'échéance de ce second délai, et sans réponse, le CERT-DEVOTEAM engagera la même procédure que celle définie en cas d'absence de point de contact (Etape 3.2), à savoir l'obtention d'un identifiant CVE et l'information du réseau des CSIRTs.

A mail will be send again at the end of that first period of 15 working days if no acknowledgement or answer has been received (Step 2.3). After an additional 15 working days without any response, CERT-DEVOTEAM will follow the same procedure as the one defined when no contact details are found, that is getting a CVE identifier and notifying the CSIRTs network (see Step 3.2).

Le CERT-DEVOTEAM, et l'éditeur, l'opérateur ou le fabricant, doivent ici partager le même objectif: définir le plus court chemin pour aboutir à la correction de la vulnérabilité et à l'information des usagers de la disponibilité d'un correctif ou d'une nouvelle version. A cette fin, le délai maximal de mise à disposition d'un correctif (Tc) sera défini et annoncé au CERT-DEVOTEAM lors de la confirmation.

CERT-DEVOTEAM and the editor, provider or manufacturer should share the same goal: defining the shortest path to get the vulnerability fully corrected, and the users' community informed of the availability of a patch or new version. To achieve this goal, a maximum period of time after which an update or a patch will be due to be made available will be defined (Tc) and announced to CERT-DEVOTEAM along with acknowledgement.

4- VALIDATION / VALIDATION

Le délai (Tc) annoncé étant écoulé, et en l'absence d'information de la part l'éditeur, l'opérateur ou le fabricant, le CERT-DEVOTEAM engagera la même procédure que celle définie en cas d'absence de point de contact (Etape 3.2), à savoir l'obtention d'un identifiant CVE et l'information du réseau des CSIRTs.

Once the pre-defined period of time for the delivery of a patch or update (Tc) has expired, and without any feedback from the editor, provider or manufacturer, CERT-DEVOTEAM will follow the same procedure as the one defined when no contact details are found, that is getting a CVE identifier and notifying the CSIRTs network (see Step 3.2).

5- PUBLICATION / PUBLICATION

L'éditeur, l'opérateur ou le fabricant, sera libre d'obtenir un identifiant CVE, et de publier son propre bulletin de sécurité. Il devra en informer le CERT-DEVOTEAM avant l'échéance du délai (Tc). Le CERT-DEVOTEAM attendra alors cette publication pour diffuser son propre avis de sécurité.

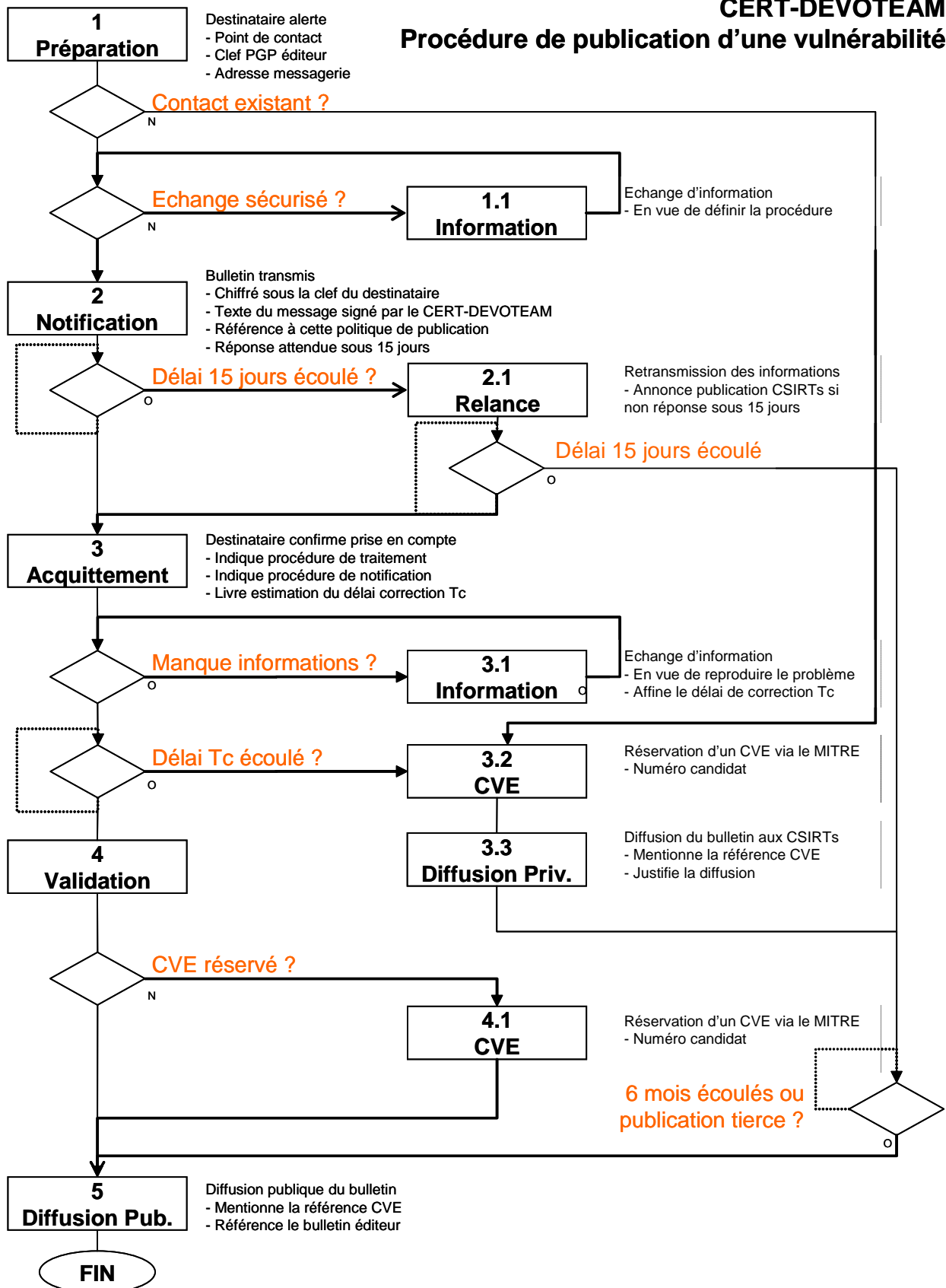
The editor, provider or manufacturer will be free to get a CVE identifier, and to publish its own security advisory. In such a case he will have to notify CERT-DEVOTEAM before the end of the delay (Tc). CERT-DEVOTEAM will then wait for this publication to send its own security advisory.

Dans l'hypothèse où aucun identifiant CVE n'aurait été réservé, le CERT-DEVOTEAM effectuera cette réservation pour son propre usage.

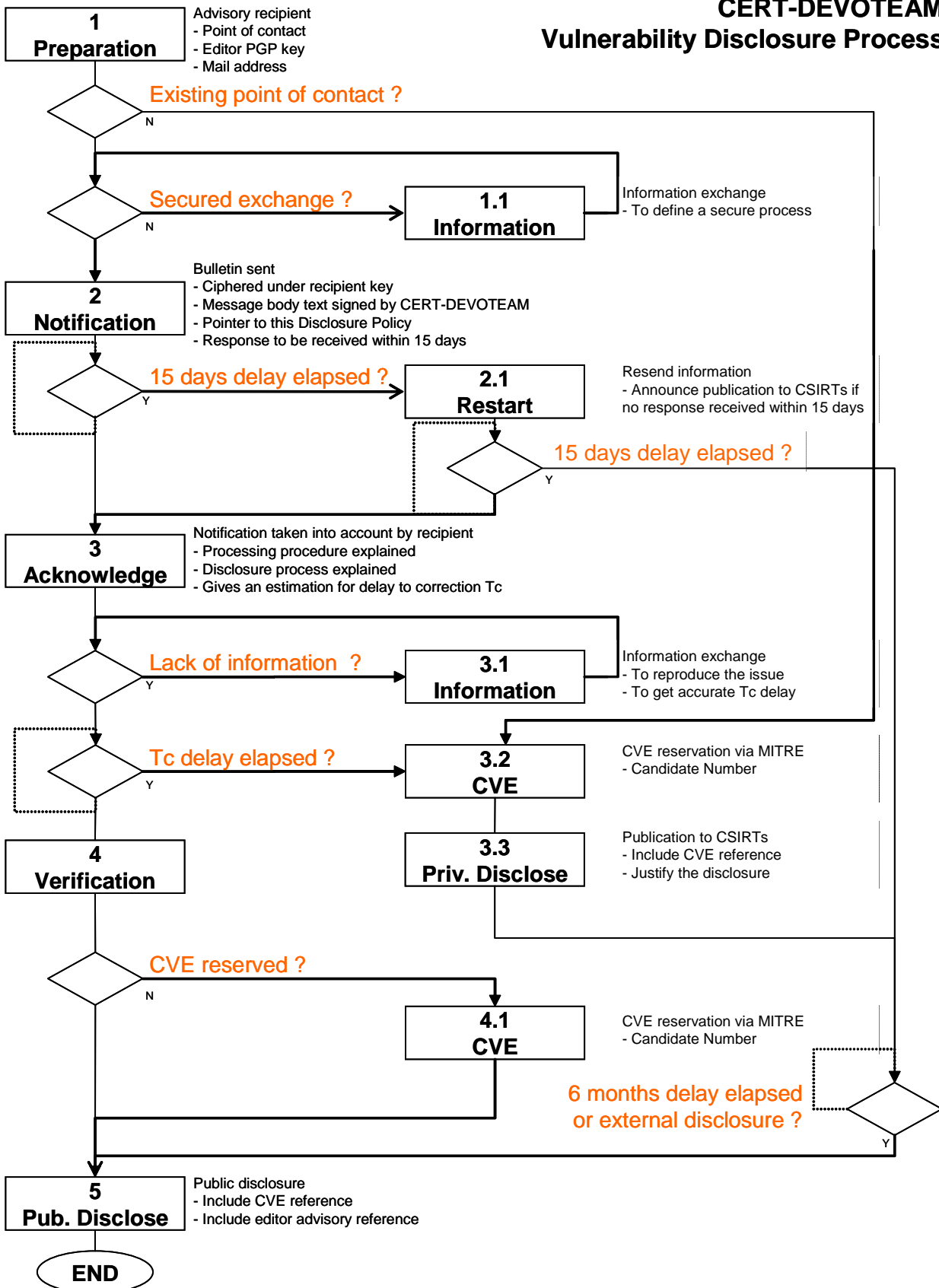
Should no CVE identifier be reserved, CERT-DEVOTEAM will go through the reservation on its own, and for its own use.

CERT-DEVOTEAM

Procédure de publication d'une vulnérabilité



**CERT-DEVOTEAM
Vulnerability Disclosure Process**



DEVOTEAM

86 rue Anatole France 92300 Levallois-Perret
Tél. : +33 (0)1 41 49 48 48 - Fax : +33 (0)1 47 57 24 76
www.devoteam.com