Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 06 décembre 2013
N° CERTA-2013-ACT-049

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTA-2013-ACT-049

1 Publication d'une note sur la mise en œuvre d'un système de journalisation

L'ANSSI a publié le 2 décembre 2013 une note technique présentant des recommandations de sécurité pour la mise en œuvre d'un système de journalisation. Les journaux sont au cœur du traitement d'incident. Ils permettent de constater rapidement des anomalies mais également a posteriori de faciliter une éventuelle investigation numérique (périmètre de compromission, domaines ou adresses IP d'exfiltration, etc.). Malheureusement le CERTA constate encore très souvent des manquements dans les procédés de journalisation mis en œuvre par les victimes (absence de synchronisation horaire, requêtes DNS non journalisées, etc.).

Ce guide aborde les prérequis à la mise en place d'un système de journalisation, à savoir :

- les fonctionnalités de journalisation ;
- l'horodatage des évènements ;
- la synchronisation des horloges ;
- le dimensionnement des ressources nécessaires à la journalisation (espaces de stockage ...).

Plusieurs recommandations d'architecture et de conception du système de journalisation sont abordées. Elles concernent notamment :

- la résilience du système de journalisation ;
- la protection des données échangées ;
- le stockage des journaux ;
- la consultation des journaux ;
- les aspects juridiques et réglementaires (conservation de données à caractère personnel, valeur probatoire des éléments conservés).

Le CERTA recommande la lecture de cette note technique et l'application des 23 recommandations identifiées.

Documentation

- Recommandations de sécurité pour la mise en œuvre d'un système de journalisation : http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-du-poste-de-travail-et-des-serveurs/recommandations-de-securite-pour-la-mise-en-oeuvre-d-un-systeme-de.html

2 Fin de support de Microsoft Windows XP et d'Office 2003

Comme évoqué dans le bulletin d'actualité CERTA-2013-ACT-016, Microsoft a planifié l'arrêt du support de Microsoft Windows XP le 08 avril 2014. A cette date, l'éditeur cessera d'assurer la publication de correctifs de sécurité pour Windows XP, y compris en cas de découverte d'une vulnérabilité critique. Il en est de même pour Microsoft Office 2003, qui cessera d'être supporté à la même date.

Actuellement deux vulnérabilités dites « 0day » touchent ces logiciels : la première (CVE-2013-3906) concerne un composant graphique de Microsoft Office et la seconde (CVE-2013-5065) le pilote `NDPROXY` de Windows XP. Si des failles similaires étaient révélées après le 08 avril 2014, Microsoft ne fournirait pas les correctifs appropriés. Les systèmes d'information utilisant encore Windows XP ou Microsoft Office resteraient alors fortement exposés aux risques de compromissions.

Le CERTA recommande donc de migrer le plus rapidement possible les systèmes Microsoft Windows XP et Microsoft Office vers des versions supportées à long terme.

Documentation

- Bulletin d'actualité CERTA-2013-ACT-016 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-ACT-016/
- Microsoft Support Lifecycle :
  http://support.microsoft.com/lifecycle/
- Bulletin d'alerte CERTA-2013-ALE-007 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-ALE-007/
- Bulletin d'alerte CERTA-2013-ALE-008 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-ALE-008/

3 Déroutage BGP

Alors que les usurpations de préfixes d'adresses IP de l'Internet sont généralement causées par des inadvertances et engendrent l'inaccessibilité des préfixes en question, des cas d'usurpations au caractère inédit ont récemment été mis en évidence par des chercheurs américains. Des attaquants sont parvenus à dévier vers la Biélorussie et l'Islande une partie du trafic IP destiné à des organisations américaines, et ce pendant plusieurs mois, sans que les utilisateurs, ni même les administrateurs réseaux, aient pu le remarquer. Bien que le but des attaques ne soit pas connu, la configuration des usurpations aurait permis l'écoute ainsi que la modification du trafic IP des victimes.

Une telle usurpation de préfixe est provoquée en exploitant le protocole de routage Internet BGP pour qu'un préfixe IP soit annoncé depuis plusieurs emplacements géographiques. En effet, les opérateurs utilisent le protocole BGP pour s'interconnecter, et ainsi, font confiance aux autres opérateurs pour router leur trafic sur Internet. Or, Internet est aujourd'hui composé de plusieurs dizaines de milliers d'opérateurs et BGP ne dispose pas de mécanisme empêchant un opérateur d'annoncer un préfixe IP qui ne lui appartient pas.

C'est pourquoi l'ANSSI recommande aux opérateurs de surveiller la bonne propagation de leurs préfixes sur Internet, et notamment de détecter l'annonce de leurs préfixes IP par des opérateurs non autorisés, pouvant mener à des usurpations de préfixes. En outre, l'ANSSI préconise la mise en oeuvre des recommandations du guide des bonnes pratiques BGP.

L'ANSSI considère l'Internet comme une infrastructure importante et évalue son bon fonctionnement au sein de l'Observatoire de la résilience de l'Internet français. Pour cela, l'Observatoire étudie plusieurs indicateurs techniques mesurables de la résilience, comme les usurpations de préfixes, dont les acteurs présents sur le territoire français sont parfois victimes.

Documentation

- Rapport de l'Observatoire pour l'année 2012 :
  http://www.ssi.gouv.fr/fr/menu/actualites/l-observatoire-sur-la-resilience-de-l-internet-francais-publie-son-rapport-2012.html
- Guide des bonnes pratiques BGP :
  http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-des-reseaux/le-guide-des-bonnes-pratiques-de-configuration-de-bgp.html

4 Comment procéder à un dépôt de plainte

Dans le cadre de sa mission de conseil et de soutien, l'ANSSI est souvent interrogée sur les modalités d'un dépôt de plainte pour des faits pouvant être interprétés comme des actes de « cyber-délinquance ».

Le dépôt de plainte est une démarche juridique positive qui permet de porter à la connaissance du procureur de la République des faits pouvant donner lieu à des poursuites pénales. Il peut être effectué soit directement auprès

du procureur de la République soit auprès d'un service de police ou de gendarmerie. Il permettra à la victime d'évaluer le préjudice subi.

Le procureur de la République décidera du service compétent pour diligenter l'enquête. Ainsi, en fonction des faits dénoncés, il pourra saisir un service spécialisé (OCLCTIC, BEFTI, DCRI, DLCC) ou des enquêteurs spécialisés présents sur toute la France. Le service saisi pourra alors constater la matérialité de l'infraction puis rechercher et identifier le ou les auteurs.

Lors du dépôt de plainte, le déclarant devra justifier de son identité. S'il s'agit d'un représentant d'une personne morale telle qu'une société, il devra également fournir un extrait Kbis de la société et un mandat émanant du représentant légal.

Afin de faciliter le traitement de la plainte il est fortement recommandé, surtout lors d'incidents complexes, de remettre au service saisi un rapport d'incident détaillé permettant de préciser :

- la nature et la date de l'attaque,
- les systèmes concernés et leur localisation géographique,
- les mesures prises pour préserver les traces et indices,
- les mesures prises en réaction à l'incident,
- l'importance du préjudice subi (durée de l'interruption de service, valeurs des données compromises, coût des opérations de remédiations, etc.),
- les coordonnées des contacts privilégiés (technicien, etc.).

Dans tous les cas, il conviendra de remettre au service de police ou de gendarmerie tous les éléments permettant de caractériser l'infraction subie et d'identifier les éventuels auteurs. Le plaignant pourra par exemple remettre, sous format électronique, des journaux d'évènements, des fichiers suspects voire des supports physiques (disques durs) ou leurs copies physiques intégrales.

Dans les cas d'affaires particulièrement complexes, le dépôt de plainte pourra être suivi par l'audition d'un technicien.

Documentation

- Les bons réflexes en cas d'intrusion sur un système d'information :
  http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-002/
- Fiches techniques - Cybercriminalité :
  http://www.securite-informatique.gouv.fr/gp_article89.html
- Porter plainte :
  http://vosdroits.service-public.fr/particuliers/F1435.xhtml

5 Rappel des avis émis

Dans la période du 29 novembre au 05 décembre 2013, le CERTA a émis les publications suivantes :

- CERTA-2013-AVI-651 : Vulnérabilité dans Apache Struts
- CERTA-2013-AVI-652 : Vulnérabilité dans VMWare
- CERTA-2013-AVI-653 : Vulnérabilité dans Xen
- CERTA-2013-AVI-654 : Multiples vulnérabilités dans Google Chrome
- CERTA-2013-AVI-655 : Vulnérabilité dans le noyau Linux

Durant la même période, les publications suivantes ont été mises à jour :

- CERTA-2005-INF-003-015 : Les systèmes et logiciels obsolètes (Actualisation et mise à jour des versions de tous les systèmes et de logiciels.)

Gestion détaillée du document

06 décembre 2013 version initiale.