Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S.G.D.S.N
Agence nationale de la sécurité des systèmes d'information
CERT-FR

Paris, le 02 mars 2015
N° CERTFR-2015-ACT-009

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2015-ACT-009

1 - DDOS HTTP par redirection DNS

Depuis janvier 2015, le CERT-FR constate des comportements réseau ayant les mêmes conséquences qu'un déni de service distribué sur certains services web. La résolution issue de certains serveurs DNS ne renvoie pas l'adresse IP correspondant au domaine demandé, mais une adresse IP aléatoire hébergeant, elle aussi, ce même service. Par exemple, un navigateur cherchant à contacter le site `www.domaine-a.com` aura comme réponse du serveur DNS l'adresse IP associée à `www.domaine-b.com`

Le CERT-FR a ainsi pu constater de très nombreuses tentatives de connexion HTTP en provenance d'AS (« *Autonomous System* ») gérés par des opérateurs de télécommunications asiatiques sur des sites français. Ces machines tentent en effet de se connecter à des systèmes n'ayant aucun rapport avec le nom de domaine qu'elles pensent contacter. Il apparaît que les noms de domaines demandés par ces clients détournés correspondent à des domaines censurés par les autorités de leur région : domaines de réseaux sociaux ou encore des domaines liés à des « trackers » utilisés pour l'échange de fichiers pair-à-pair.

Lors de ces analyses, le CERT-FR n'a pas pu faire de lien entre les domaines d'origine et les adresses effectivement contactés. Ce phénomène est constaté par d'autres acteurs. Les victimes doivent alors faire face à d'importants flux de données non planifiés.

Les recommandations contre les attaques par déni de service du CERT-FR s'appliquent et sont disponibles à l'adresse :

– http://www.cert.ssi.gouv.fr/site/CERTA-2012-INF-001/CERTA-2012-INF-001.html

D'autres analyses sont disponibles ici :

– http://www.bortzmeyer.org/sichuan-pepper.html
– https://isc.sans.edu/forums/diary/Are+You+thepiratebayorg+Resolving+to+Various+Hosts/19175/

2 - Vulnérabilité dans le code de Samba

Description de la vulnérabilité

Samba est un outil, fonctionnant sur les systèmes Linux et Unix, permettant de partager des dossiers et des imprimantes à travers un réseau local, en implémentant le protocole de communication SMB/CIFS utilisé par Microsoft Windows.

Le 23 février 2015, l'éditeur de Samba a publié sur son site un avis de sécurité concernant une vulnérabilité identifiée par la CVE-2015-0240. Cette vulnérabilité, située dans la partie serveur de Samba (`smbd`), permettrait une exécution de code arbitraire à distance en tant que super-utilisateur et sans authentification préalable.

Un attaquant pourrait, en forgeant des paquets, atteindre un chemin d'exécution spécifique où une structure est libérée sans avoir été précédemment allouée.

En effet, la fonction `_netr_ServerPasswordSet` déclare un pointeur vers une structure de type `netlogon_creds_CredentialState` sur sa pile (1) qui est ensuite passé à la fonction `netr_creds_server_step_check` (2).

Si le résultat de cet appel n'est pas valide, alors la mémoire allouée pour la structure dans la fonction `netr_creds_server_step_check` est libérée par un appel à `TALLOC_FREE` (3).

```
NTSTATUS _netr_ServerPasswordSet(struct pipes_struct *p,
    struct netr_ServerPasswordSet *r) {
        NTSTATUS status = NT_STATUS_OK;
        int i;
    (1) struct netlogon_creds_CredentialState *creds;
        become_root();
    (2) status = netr_creds_server_step_check(p, p->mem_ctx,
            r->in.computer_name,
            r->in.credential,
            r->out.return_authenticator,
            &creds);
        unbecome_root();
        if (!NT_STATUS_IS_OK(status)) {
    (3)     TALLOC_FREE(creds);
            return status;
        }
        [...]
}
```

Dans la fonction `netr_creds_server_step_check`, il est possible d'éviter l'allocation mémoire effectuée par `schannel_check_creds_state` (3) en faisant échouer la fonction `schannel_check_required` (2).

L'appel à cette fonction dépend de la valeur de `schannel_global_required`, qui provient du paramètre global `server schannel` du fichier de configuration `smb.conf` (1). Il est à noter que, par défaut, cette valeur est telle que l'appel à `schannel_check_required` (2) est effectué.

```
static NTSTATUS netr_creds_server_step_check(struct pipes_struct *p,
    [...]
    struct netlogon_creds_CredentialState **creds_out) {
        NTSTATUS status;
    (1) bool schannel_global_required = (lp_server_schannel() == true) ? true:false;
        struct loadparm_context *lp_ctx;
        if (schannel_global_required) {
    (2)     status = schannel_check_required(&p->auth,
                computer_name,
                false, false);
            if (!NT_STATUS_IS_OK(status)) {
                return status;
            }
        }
        [...]
    (3) status = schannel_check_creds_state(mem_ctx, lp_ctx,
            computer_name, received_authenticator,
            return_authenticator, creds_out);
        [...]
}
```

Pour faire échouer l'appel à `schannel_check_required`, il "suffit" que la valeur `p->auth_info->auth_type`, contrôlée par l'attaquant, soit différente de `DCERPC_AUTH_TYPE_SCHANNEL`.

```
static NTSTATUS schannel_check_required(struct pipe_auth_data *auth_info,
    const char *computer_name,
    bool integrity, bool privacy){
        if (auth_info && auth_info->auth_type == DCERPC_AUTH_TYPE_SCHANNEL) {
        [...]
        }
        return NT_STATUS_ACCESS_DENIED;
}
```

Samba utilise un gestionnaire de mémoire. Ce dernier dispose d'une fonctionnalité permettant d'effectuer un appel à un destructeur lors de la libération de mémoire. Lors de l'appel à `TALLOC_FREE`, la fonction `_talloc_free_internal` est exécutée. C'est cette dernière qui est responsable de l'appel au destructeur :

```
static inline int _talloc_free_internal(void *ptr, const char *location) {
    [...]
    tc = talloc_chunk_from_ptr(ptr);
    [...]
    if (unlikely(tc->destructor)) {
        talloc_destructor_t d = tc->destructor;
        [...]
        if (d(ptr) == 1) {
            tc>destructor = d;
            return 1;
        }
        tc>destructor = NULL;
    }
    [...]
}
```

Si l'attaquant est en mesure de contrôler les données positionnées à l'adresse pointée par `creds`, alors il peut contrôler la valeur du destructeur et ainsi aboutir à une exécution de code arbitraire.

Correctif de sécurité

Afin de corriger cette vulnérabilité, un correctif a été publié par l'éditeur. En affectant la valeur `NULL` au pointeur `creds` lors de sa déclaration, il devient alors impossible pour l'attaquant de contrôler les données pointées.

Depuis la publication de l'avis de sécurité, ce correctif aété intégré par toutes les distributions majeures de Linux. Même si, jusqu'à présent, aucun code d'exploitation de cette vulnérabilité n'a été rendu public, le CERT-FR recommande à ses lecteurs l'application au plus tôt des correctifs ou la mise à jour, via le gestionnaire de logiciels de la distribution, de Samba.

Documentation

- Avis Samba :
  https://www.samba.org/samba/security/CVE-2015-0240
- Avis du CERT-FR :
  http://www.cert.ssi.gouv.fr/site/CERTFR-2015-AVI-078/CERTFR-2015-AVI-078.html
- Analyse de RedHat :
  https://securityblog.redhat.com/2015/02/23/samba-vulnerability-cve-2015-0240/

3 - Rappel des avis émis

Dans la période du 23 février au 01 mars 2015, le CERT-FR a émis les publications suivantes :

- CERTFR-2015-AVI-077 : Vulnérabilité dans Cisco IOS
- CERTFR-2015-AVI-078 : Vulnérabilité dans Samba
- CERTFR-2015-AVI-079 : Multiples vulnérabilités dans les produits Mozilla
- CERTFR-2015-AVI-080 : Vulnérabilité dans Huawei iMana
- CERTFR-2015-AVI-081 : Multiples vulnérabilités dans le noyau Linux d'Ubuntu

Gestion détaillée du document

02 mars 2015 version initiale.

Conditions d'utilisation de ce document :	`http://cert.ssi.gouv.fr/cert-fr/apropos.html`
Dernière version de ce document :	`http://cert.ssi.gouv.fr/site/CERTFR-2015-ACT-009`