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 24 octobre 2016
N° CERTFR-2016-ACT-043

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2016-ACT-043

1 - Dirty Cow

Depuis mercredi dernier, la vulnérabilité CVE-2016-5195 est publique. L'exploitation de celle-ci conduit à une élévation de privilège et donc de disposer de droits privilégiés (root) sur un système. Afin d'être exploitée, un attaquant doit disposer d'un accès à un compte utilisateur (non-privilégié) sur un système Linux. Cet accès peut soit être légitime, soit être obtenu grâce à une autre vulnérabilité exploitée préalablement. L'aspect distant ou local de l'accès au compte utilisateur n'a pas d'incidence sur son exploitation.

Du fait de l'utilisation massive de Linux, de très nombreux systèmes sont potentiellement vulnérables, tels que la majorité des serveurs web sur internet, les ordiphones fonctionnant sur le système d'exploitation Android ou encore de nombreux équipements réseau.

À titre d'exemple, les systèmes de gestion de contenu (Content Management Systems) sont régulièrement vulnérables à des failles permettant d'exécuter du code à distance. Cela permet d'obtenir l'accès à un compte non privilégié, utilisable pour exploiter la vulnérabilité CVE-2016-5195.

Le découvreur a également publié plusieurs preuves de concept exploitant la vulnérabilité. La facilité et la fiabilité d'exécution de ces codes imposent une attention particulière sur la CVE-2016-5195.

Détails de la vulnérabilité

Cette vulnérabilité est présente dans le noyau Linux depuis la version 2.6.22 dont la sortie date de 2007. Linus Torvalds indique qu'une correction de ce bogue a été tentée il y a 11 ans, mais avait été abandonné pour des raisons de compatibilité avec du matériel Intel. À l'époque, cette attaque était considérée plus théorique que pratique.[1] Le chercheur qui l'a rendue publique, Phil Oester, a nommé cette vulnérabilité `Dirty Cow`[2]. Dirty Cow est déclenchée par une situation de compétition (ou 'race condition') dans le mécanisme de copie à l'occasion d'une écriture en mémoire ('Copy on Write' ou 'cow'). Dans un souci d'optimisation des ressources, une projection en mémoire (memory mapping) peut être créée afin qu'elles soient accessibles à plusieurs processus. Lorsque l'un de ces processus souhaite écrire pour modifier les données, cette page est copiée et la nouvelle page est considérée comme sale (ou 'dirty'). Cela indique qu'elle a changé et que le système devra écrire cette page sur le disque. Ce mécanisme permet de limiter les entrées/sorties sur le disque, car ces opérations sont les plus coûteuses. Il existe plusieurs preuves de concept qui fonctionnent globalement de la manière suivante :

- un exécutable appartenant au super-utilisateur est ouvert alors que l'utilisateur ne dispose que des droits en lecture ;
- une projection en mémoire de cet exécutable est réalisée grâce à la fonction `mmap()` [3] ;
- deux autres fils d'exécution doivent ensuite être lancés. Le premier appelle `madvise()`[4] en boucle avec l'argument `MADV_DONTNEED` ce qui permet d'indiquer au système que la page ne sera plus utilisée. Dans le deuxième fil, un fichier en lecture/écriture pouvant examiner son état interne (par exemple `/proc/self/mem` ou `ptrace`) est ouvert.

Lors d'une tentative d'écriture sur une page par le deuxième fil, une copie est crée (ce qui prend un certain temps, même minime), la nouvelle page est marquée comme sale. Le premier fil appelle la fonction `madvise()` avec

l'argument `MADV_DONTNEED`. Le système libère la nouvelle page sans écrire sur le disque car l'utilisateur n'a pas les droits en écriture sur la page initiale. Il s'agit du comportement attendu. Or, tenter cette opération de manière répétée conduit potentiellement à un cas limite où l'écriture en mémoire se produit avant que la table des pages ne se soit mise à jour pour pointer vers la copie. Cette erreur débouche sur une écriture sur la page originale pour laquelle l'utilisateur n'avait les droits qu'en lecture. Même si la probabilité de se retrouver dans cette situation est faible, M. Oester estime le temps pour déclencher cette vulnérabilité est inférieur à 5 secondes[5], ce qui rend l'exploitation de Dirty Cow rapide et peu coûteuse.

Recommandations

Certaines distributions comme Ubuntu[6], Red Hat[7] ou encore Suse[8] proposent des correctifs, mais ce n'est pas le cas de toutes. De nombreux autres éditeurs dont les solutions reposent également sur un noyau Linux proposeront des correctifs. Le CERT-FR recommande de veiller à l'application de ces correctifs de sécurité dès qu'ils sont disponibles. Enfin, de nombreux autres systèmes vulnérables ne disposeront pas de correctifs, il convient d'identifier ces systèmes, les risques associés et de mettre en oeuvre des contre-mesures.

Documentation

1 Message Linus Torvalds
https://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=19be0eaffa3ac7d8eb6784ad9bdbc7d67ed8e619
2 Dirty Cow
http://dirtycow.ninja/
3 Mmap()
http://man7.org/linux/man-pages/man2/mmap.2.html
4 Madvise()
http://man7.org/linux/man-pages/man2/madvise.2.html
5 article ars technica
http://arstechnica.com/security/2016/10/most-serious-linux-privilege-escalation-bug-ever-is-under-active-exploit/
6 Avis CERTFR-2016-AVI-353
http://www.cert.ssi.gouv.fr/site/CERTFR-2016-AVI-353
7 Avis CERTFR-2016-AVI-356
http://www.cert.ssi.gouv.fr/site/CERTFR-2016-AVI-356
8 Avis CERTFR-2016-AVI-357
http://www.cert.ssi.gouv.fr/site/CERTFR-2016-AVI-357
– Référence CVE CVE-2016-5195
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5195

2 - Rappel des avis émis

Dans la période du 17 au 23 octobre 2016, le CERT-FR a émis les publications suivantes :

– CERTFR-2016-AVI-348 : Multiples vulnérabilités dans Oracle Database Server
– CERTFR-2016-AVI-349 : Multiples vulnérabilités dans Oracle Java SE
– CERTFR-2016-AVI-350 : Multiples vulnérabilités dans Oracle Linux and Virtualization
– CERTFR-2016-AVI-351 : Multiples vulnérabilités dans Oracle MySQL
– CERTFR-2016-AVI-352 : Multiples vulnérabilités dans SCADA les produits Schneider
– CERTFR-2016-AVI-353 : Multiples vulnérabilités dans le noyau Linux d'Ubuntu
– CERTFR-2016-AVI-354 : Multiples vulnérabilités dans les produits Cisco
– CERTFR-2016-AVI-355 : Multiples vulnérabilités dans Mozilla Firefox

Gestion détaillée du document

24 octobre 2016 version initiale.