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 06 juillet 2015
N° CERTFR-2015-ACT-027

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2015-ACT-027

1 - Revue d'HTTP/2

Introduction

Le standard *Hyper Text Transfer Protocol* est utilisé depuis les années 90 pour la navigation sur internet. En 2012, un groupe de travail s'est mis en place pour en améliorer la sécurité et la vitesse des échanges utilisant ce protocole. La dernière mise à jour de la version la plus couramment utilisée - HTTP 1.1 - a été publiée en juin 2014.

En se basant sur la technologie SPDY, développée par Google, le groupe de travail a mis au point HTTP/2, dont une première version a été approuvée par l'IETF le 18 février 2015.

Fonctionnalités

Cette nouvelle version de HTTP cherche à améliorer l'efficacité, la vitesse et la sécurité des échanges sur internet sans changer complètement le fonctionnement du protocole. Les motivations principales du groupe de travail sont l'optimisation de l'usage des ressources du réseau, l'amélioration de la sécurité ainsi que des réponses aux problèmes de HTTP/1.1.

Pour accomplir ces tâches, plusieurs fonctionnalités sont ajoutées. Sont notamment à citer l'utilisation d'un protocole binaire, le multiplexage, l'envoi de plusieurs ressources à travers une seule connexion TCP, la possibilité pour le serveur de pousser des données au client et la compression des en-têtes.

Rétrocompatibilité

L'en-tête `Upgrade` peut être utilisé par le client pour signifier une volonté de passer à HTTP/2 pour les communications. Un serveur compatible uniquement avec des versions précédentes de HTTP ignorera automatiquement cet en-tête et la communication continuera sur l'ancien protocole.

Le fait que HTTP/2 soit un protocole binaire nécessite un gros travail d'adaptation pour de nombreux logiciels. Certains sont d'ores et déjà préparés, comme l'outil Wireshark qui peut analyser ce protocole.

Le CERT-FR recommande de mettre à jour les logiciels de journalisation réseau, les versions récentes de ces derniers étant plus propices à supporter HTTP/2.

Sécurité

Chiffrement

HTTP/2 impose des contraintes sur les suites de chiffrement à utiliser. L'échange chiffré doit – a minima – utiliser TLS 1.2. Les spécifications actuelles du protocole HTTP/2 ne forcent pas le chiffrement des données, cependant certaines implémentations actuelles ne proposent le protocole HTTP/2 que pour des connexions chiffrées.

Une des nouvelles fonctionnalités du protocole est la possibilité de proposer des services alternatifs, un entête `Alt-Svc` permet ainsi d'indiquer au client de se connecter en utilisant un autre protocole ou un autre port. De cette façon, il est étudié la mise en place de chiffrement opportuniste permettant à un client – si le serveur le propose – de chiffrer avec TLS la communication, même en HTTP. Une telle fonctionnalité permet de se protéger contre les écoutes clandestines de ladite communication, mais pas d'authentifier le serveur.

Failles et mitigations

La compression dans des flux chiffrés a été la source de plusieurs attaques comme CRIME ou BREACH. Les spécifications de HTTP/2 et la méthode de compression HPACK ont été pensées pour que le langage ne présente plus les mêmes vulnérabilités.

Mozilla a dû désactiver en avril le chiffrement opportuniste, qui permettait alors l'exploitation d'une vulnérabilité critique permettant une situation de singe intercepteur sur des connexions chiffrées.

Plus récemment, une équipe de chercheurs a mis en avant des vulnérabilités liées à l'implémentation de HTTP/2 dans Apache Traffic Server.

Le CERT-FR recommande dans la phase transitoire de renforcement du protocole d'éviter la mise en production au regard des failles régulièrement trouvées.

Logiciels supportant HTTP/2

Les systèmes suivants supportent le protocole :
- le serveur mandataire Squid à partir de la version 4 (en cours d'élaboration) ;
- cURL supporte certaines fonctionnalités de HTTP/2 à l'aide de la librairie nghttp2 ;
- Wireshark possède un dissecteur pour HTTP/2 ;
- iOS9 (Apple) est un client HTTP/2 (le navigateur aussi bien que les applications) ;
- les pages d'accueil de Google et Twitter sont accessibles en HTTP/2.

Documentation

- RFC 7540 sur HTTP/2 (en anglais) :
  https://httpwg.github.io/specs/rfc7540.html
- RFC 7541 sur HPACK (en anglais) :
  https://httpwg.github.io/specs/rfc7541.html
- Démonstration de variation de performances :
  https://http2.akamai.com/demo
- Chiffrement opportuniste - proposition (en anglais) :
  http://httpwg.github.io/http-extensions/encryption.html
- Retour du CERT-FR sur CRIME :
  http://www.cert.ssi.gouv.fr/site/CERTA-2012-ACT-042/
- Présentation de BREACH (en anglais) :
  http://breachattack.com/resources/BREACH - SSL, gone in 30 seconds.pdf
- Vulnérabilité dans Mozilla Firefox :
  https://www.mozilla.org/en-US/security/advisories/mfsa2015-44/
- Vulnérabilité dans Apache Traffic Server :
  http://yahoo-security.tumblr.com/post/122883273670/apache-traffic-server-http2-fuzzing

2 - Fin de support de Microsoft Windows 2003

Microsoft a planifié l'arrêt du support de Microsoft Windows 2003 le **14 juillet 2015**. À cette date, l'éditeur cessera d'assurer la publication de correctifs de sécurité, y compris en cas de découverte d'une vulnérabilité critique.

En ce qui concerne le système d'exploitation Windows 2003, un grand nombre de mécanismes de sécurité sont absents, à l'inverse de Windows 8 ou Windows 7. L'absence de tels mécanismes facilite la prise de contrôle par un attaquant à l'aide de techniques d'exploitation largement diffusées.

Il est important de souligner que l'arrêt du support de Windows 2003 va entraîner une recrudescence des codes d'exploitation de vulnérabilité de type « 0-day » dans les kits d'exploitation. Les vendeurs de vulnérabilités vont

probablement en profiter pour écouler leur réserve de « 0-day ». Ces vulnérabilités auront plus de valeur pour les attaquants dans la mesure où elles ne seront pas corrigées par l'éditeur.

Le support et la mise à disposition de mises à jour de sécurité par l'éditeur sont un point crucial à la sécurisation d'un serveur ou d'une station de travail. L'arrêt du support d'une version de système d'exploitation doit être anticipé et constitue une motivation à la migration vers une version récente. Cela concerne en majorité les postes de travail mais peut également concerner des équipements intégrés embarquant le système Windows 2003 (ex : équipements industriels, médicaux, interfaces utilisateur, etc...). Pour ces derniers, pouvant faire l'objet de contraintes métier, une démarche spécifique doit être engagée, en coordination avec le fournisseur, afin d'étudier les différents scenarios envisageables.

De plus, la durée de vie du système d'exploitation retenu pour la migration doit être adaptée au cycle de vie des projets et à la vitesse de renouvellement du parc informatique. Une période de cinq ans minimum est recommandée pour les environnements bureautiques.

De nombreux systèmes utilisant Microsoft Windows 2003 sont aujourd'hui encore en service dans les administrations et les entreprises. Le CERT-FR attire l'attention sur la nécessité d'anticiper dès à présent une migration vers des systèmes dont la pérennité des mises à jour de sécurité pourra être assurée après cette date.

3 - Rappel des avis émis

Dans la période du 29 juin au 05 juillet 2015, le CERT-FR a émis les publications suivantes :

- CERTFR-2015-AVI-268 : Multiples vulnérabilités dans les produits Citrix Netscaler
- CERTFR-2015-AVI-269 : Vulnérabilité dans le noyau Linux de Fedora
- CERTFR-2015-AVI-270 : Vulnérabilité dans Schneider SCADA SAGE Remote Terminal Units
- CERTFR-2015-AVI-271 : Multiples vulnérabilités dans Apple Mac EFI
- CERTFR-2015-AVI-272 : Multiples vulnérabilités dans Apple iOS
- CERTFR-2015-AVI-273 : Multiples vulnérabilités dans Apple OSX
- CERTFR-2015-AVI-274 : Multiples vulnérabilités dans Apple Quicktime
- CERTFR-2015-AVI-275 : Multiples vulnérabilités dans Apple iTunes
- CERTFR-2015-AVI-276 : Multiples vulnérabilités dans Apple Safari
- CERTFR-2015-AVI-277 : Vulnérabilité dans BlueCoat Malware Analysis Appliance
- CERTFR-2015-AVI-278 : Vulnérabilité dans Cisco Unified Communications Domain Manager
- CERTFR-2015-AVI-279 : Multiples vulnérabilités dans les produits Mozilla

Gestion détaillée du document

06 juillet 2015 version initiale.