Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 29 novembre 2010
N° CERTA-2009-AVI-482-011

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du protocole SSL/TLS

Gestion du document

Référence	CERTA-2009-AVI-482-011
Titre	Vulnérabilité du protocole SSL/TLS
Date de la première version	06 novembre 2009
Date de la dernière version	29 novembre 2010
Source(s)	–
Pièce(s) jointe(s)	Aucune

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

Contournement de la politique de sécurité.

2 Systèmes affectés

- OpenSSL versions antérieures à 0.9.8l ;
- Sun Java Enterprise System Suite (voir le bulletin de sécurité Sun du 11 janvier 2010) ;
- IBM WebSphere DataPower SOA appliances (voir le bulletin de sécurité IBM du 11 janvier 2010) ;
- IBM multiples implémentations de SSL/TLS (voir le bulletin de sécurité IBM du 13 janvier 2010).

D'autres implémentations du protocole sont probablement touchées, ainsi que des applications utilisant OpenSSL.

3 Résumé

Une vulnérabilité dans le protocole SSL/TLS permet à une personne malintentionnée de contourner la politique de sécurité.

4 Description

Une vulnérabilité a été identifiée dans le protocole SSL/TLS lors de renégociations de sessions. Une personne s'étant au préalable mise en situation « d'homme au milieu » (*man in the middle*) peut, dans certaines circonstances, injecter des données à l'encontre d'un utilisateur, pour, par exemple, forcer l'envoi d'une requête HTTP au serveur vers lequel la victime se connecte.

5 Solution

La version 0.9.8l de OpenSSL désactive la renégociation de sessions par défaut.

6 Documentation

- Mise à jour de OpenSSL :
  http://www.openssl.org/source/
- Bulletin de sécurité Apple HT4004 du 19 janvier 2010 :
  http://support.apple.com/kb/HT4004
- Bulletin de sécurité Bluecoat SA44 du 23 février 2010 :
  http://kb.bluecoat.com/index?page=content&id=SA44
- Bulletin de sécurité Cisco cisco-sa-20091109-tls du 26 février 2010 :
  http://www.cisco.com/warp/public/707/cisco-sa-20091109-tls.shtml
- Bulletin de sécurité Cisco cisco-sa-20091109-tls du 22 juillet 2010 :
  http://www.cisco.com/en/US/products/products_security_advisory09186a0080b01d1d.shtml
- Bulletin de sécurité Debian DSA 1934 du 16 novembre 2009 :
  http://www.debian.org/security/2009/dsa-1934
- Bulletins de sécurité Fedora FEDORA-2009-12229 et 12305 du 27 novembre 2009 :
  https://www.redhat.com/archives/fedora-packages-announce/2009-December/msg01029.html
  https://www.redhat.com/archives/fedora-packages-announce/2009-December/msg01020.html
- Bulletins de sécurité Fedora FEDORA-2009-12604 et 12606 du 04 décembre 2009 :
  https://www.redhat.com/archives/fedora-packages-announce/2009-December/msg00645.html
  https://www.redhat.com/archives/fedora-packages-announce/2009-December/msg00944.html
- Bulletins de sécurité Fedora FEDORA-2009-12750, 12775 et 12782 du 07 décembre 2009 :
  https://www.redhat.com/archives/fedora-packages-announce/2009-December/msg00428.html
  https://www.redhat.com/archives/fedora-packages-announce/2009-December/msg00442.html
  https://www.redhat.com/archives/fedora-packages-announce/2009-December/msg00449.html
- Bulletin de sécurité Gentoo GLSA-200912-01 du 02 décembre 2009 :
  http://www.gentoo.org/security/en/glsa/glsa-200912-01.xml
- Bulletin de sécurité HP c01945686 du 12 décembre 2009 :
  http://h20000.www2.hp.com/bizsupport/TechSupport/Documents.jsp?objectID=c01945686
- Bulletin de sécurité HP c02171256 du 17 mai 2010 :
  http://h20000.www2.hp.com/bizsupport/TechSupport/Documents.jsp?objectID=c02171256
- Bulletin de sécurité IBM du 11 janvier 2010 :
  http://www-01.ibm.com/support/docview.wss?uid=swg21390112
- Bulletin de sécurité IBM du 13 janvier 2010 :
  http://www-01.ibm.com/support/docview.wss?uid=nas258cbfcf0a5645af7862576710041f65e
- Bulletin de sécurité IBM du 22 janvier 2010 pour IBM WebSphere :
  http://www-01.ibm.com/support/docview.wss?uid=swg24025718
- Bulletin de sécurité IBM du 27 janvier 2010 pour IBM WebSphere :
  http://www-01.ibm.com/support/docview.wss?uid=swg24025719
- Bulletin de sécurité IBM du 25 novembre 2010 pour IBM WebSphere MQ :
  http://www-01.ibm.com/support/docview.wss?uid=swg24006386
- Bulletin de sécurité Microsoft MS10-049 du 10 août 2010 :
  http://www.microsoft.com/france/technet/security/Bulletin/MS10-049.mspx
  http://www.microsoft.com/technet/security/Bulletin/MS10-049.mspx

- Bulletins de sécurité OpenBSD du 26 novembre 2009 :
  http://openbsd.org/errata45.html#010_openssl
  http://openbsd.org/errata46.html#004_openssl
- Bulletin de version ProFTPd 1.3.2c :
  http://www.proftpd.org/docs/RELEASE_NOTES-1.3.2c
- Bulletins de sécurité RedHat RHSA-2009:1579 et 1580 du 11 novembre 2009 :
  http://rhn.redhat.com/errata/RHSA-2009-1579.html
  http://rhn.redhat.com/errata/RHSA-2009-1580.html
- Bulletins de sécurité RedHat RHSA-2010:0162 à 0167 du 25 mars 2010 :
  http://rhn.redhat.com/errata/RHSA-2010-0162.html
  http://rhn.redhat.com/errata/RHSA-2010-0163.html
  http://rhn.redhat.com/errata/RHSA-2010-0164.html
  http://rhn.redhat.com/errata/RHSA-2010-0165.html
  http://rhn.redhat.com/errata/RHSA-2010-0166.html
  http://rhn.redhat.com/errata/RHSA-2010-0167.html
- Bulletin de sécurité RedHat RHSA-2010:0173 du 25 mars 2010 :
  http://rhn.redhat.com/errata/RHSA-2010-0173.html
- Bulletin de sécurité Sun du 19 novembre 2009 :
  http://sunsolve.sun.com/search/document.do?assetkey=1-66-273029-1
- Bulletin de sécurité Sun du 11 janvier 2010 :
  http://sunsolve.sun.com/search/document.do?assetkey=1-66-274990-1
- Bulletin de sécurité SUSE SUSE-SA:2009:057 du 18 novembre 2009 :
  http://lists.opensuse.org/opensuse-security-announce/2009-11/msg00009.html
- Référence CVE CVE-2009-3245 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3245
- Référence CVE CVE-2009-3555 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3555

Gestion détaillée du document

06 novembre 2009 version initiale.

27 novembre 2009 ajout du bulletin de sécurité Sun du 19 novembre 2009.

11 janvier 2010 ajout du bulletin de sécurité Sun du 11 janvier 2010.

13 janvier 2010 ajout du bulletin de sécurité IBM du 11 janvier 2010.

14 janvier 2010 ajout du bulletin de sécurité IBM du 13 janvier 2010.

27 janvier 2010 ajout des bulletins de sécurité IBM du 22 et 27 janvier 2010.

04 mars 2010 ajout des bulletins de sécurité Apple, Bluecoat, Cisco, Debian, Fedora, Gentoo, openBSD, ProFTPd, RedHat et Suse.

26 mars 2010 ajout des bulletins de sécurité RedHat et de la référence CVE-2009-3245.

19 mai 2010 ajout des bulletins de sécurité HP.

29 juillet 2010 ajout du bulletin Cisco.

11 août 2010 ajout du bulletin Microsoft.

29 novembre 2010 ajout du bulletin IBM WebSphere MQ.