Heartbleed

Heartbleed est une vulnérabilité logicielle présente dans la bibliothèque de cryptographie open source OpenSSL à partir de mars 2012, qui permet à un « attaquant » de lire la mémoire d'un serveur ou d'un client pour récupérer, par exemple, les clés privées utilisées lors d'une communication avec le protocole Transport Layer Security (TLS). Découverte en mars 2014 et rendue publique le 7 avril 2014, elle concerne de nombreux services Internet. Ainsi 17 % des serveurs web dits sécurisés, soit environ un demi-million de serveurs, seraient touchés par la faille au moment de la découverte du bogue[1].

Symbole utilisé pour communiquer au sujet de la vulnérabilité Heartbleed.

Sommaire

- Histoire
- Conséquences
- Versions vulnérables
- Services et logiciels affectés
  - Sites internet
  - Applications
  - Systèmes d'exploitation
- Notes et références
- Annexes
  - Articles connexes
  - Liens externes

Histoire

La vulnérabilité aurait été introduite par erreur[2] dans le référentiel d'OpenSSL, à la suite d'une proposition de correction de bugs et d'améliorations de fonctionnalités, par un développeur bénévole[2,3]. La proposition a été examinée et validée par l'équipe d'OpenSSL le 31 décembre 2011[4], et le code vulnérable a été ajouté dans la version 1.0.1 d'OpenSSL, le 14 mars 2012[5,6,7].

En avril 2014, le bug a été découvert, de manière indépendante, par l'équipe sécurité de Google et par des ingénieurs de la société finlandaise Codenomicon[8,7].

Conséquences

Cette faille pourrait permettre à des internautes mal intentionnés de récupérer des informations situées sur les serveurs d'un site vulnérable, à l'insu de l'utilisateur qui les possède. Ces informations personnelles sont censées être inaccessibles et protégées, mais cependant plusieurs experts ont retrouvé des mots de passe d'utilisateurs de sites victimes. Néanmoins, un informaticien de Google ayant participé à la correction de la faille reste plus mesuré et écrit n'avoir vu que des informations parcellaires ou ne pas avoir vu d'informations sensibles[9].

La vulnérabilité a mis en évidence le manque de moyens des logiciels libres tels que OpenSSL et a mené à un projet de financement groupé de ces derniers par de nombreuses entreprises majeures (Amazon Web Services, Microsoft, Google, Facebook, etc.). Ce projet commun est nommé Core Infrastructure Initiative[10, 11, 12].

Les résultats d'audit semblent montrer que certains « attaquants » peuvent avoir exploité la faille pendant au moins cinq mois avant qu'elle ne soit officiellement découverte et corrigée[13, 14].

Les appareils sous Android 4.1.1 sont concernés par la faille, soit un peu moins de 10 % des appareils actifs[15].

L'influence possible de la faille a d'abord été abordé par le principe de précaution, de nombreux sites demandant à leurs utilisateurs de changer leur mot de passe après avoir appliqué les mises à jour de sécurité. Le 11 avril 2014, CloudFlare explique que ses spécialistes en sécurité n'ont pas réussi à exploiter la faille pour extraire des clés de sécurité SSL, en déduisant que les risques encourus sont peut-être moins importants que prévu[16]. Pour le vérifier l'entreprise lance un concours d'exploitation de la faille, qui est remporté dans la journée par deux personnes[17].

Selon Bloomberg, la National Security Agency (NSA) a exploité la faille pendant au moins deux ans, pour des opérations de surveillance et d'espionnage[18]. L'agence dément le jour même[19].

Des experts, dont Johannes Ullrich du SANS Institute, indiquent que la mise à jour des certificats de sécurité des navigateurs web ralentirait l'accès à certains sites[20].

Le site de Filippo Valsorda permet de tester si un site est vulnérable ou non[9].

Versions vulnérables

- Les versions antérieures (0.9.8 et 1.0.0) d'OpenSSL ne sont pas vulnérables à ce bug[7].
- Les versions 1.0.1 (disponibles depuis décembre 2011) à 1.0.1f (incluse) d'OpenSSL sont vulnérables[7].
- La version 1.0.1g disponible depuis le 7 avril 2014 corrige le bug[7].

Services et logiciels affectés

Sites internet

Les sites suivants ont été affectés ou ont fait des annonces recommandant à leurs utilisateurs de changer leurs mots de passe, à la suite du bug :

- Akamai Technologies[21]
- Amazon Web Services[22]
- Ars Technica[23]
- Bitbucket[24]
- BrandVerity[25]
- Freenode[26]
- GitHub[27]
- IFTTT[28]
- Internet Archive[29]
- Mojang[30]
- Mumsnet[31]
- Peerj[32]
- Pinterest[33]
- Prezi[34]
- Reddit[35]
- Something Awful[36]
- SoundCloud[37]
- SourceForge[38]
- SparkFun[39]
- Stripe[40]
- Tumblr[41, 42]
- Wattpad[réf. nécessaire]
- Wikimédia (incluant Wikipédia)[43]
- Wunderlist[44]

Applications

De nombreuses applications sont affectées par ce bug. Les éditeurs fournissent des mises à jour, par exemple :

- IPCop a publié le 8 avril 2014 une version 2.1.4a afin de corriger le bug[45] ;
- L'application de gestion de mots de passe en ligne LastPass Password Manager **(en)** ;
- LibreOffice 4.2.3 publiée le 10 avril 2014[46] ;
- LogMeIn indique proposer la mise à jour de nombreux produits qui reposaient sur OpenSSL[47] ;
- Serveurs d'applications HP[48] ;
- McAfee[49] ;
- VMware series[50].

Des services de jeux en ligne comme Steam, Minecraft, League of Legends, GOG.com, Origin Systems, Secret of Evermore, Humble Bundle, et Path of Exile sont aussi affectés[51].

Systèmes d'exploitation

- Android 4.1.1 (Jelly Bean), utilisé dans de nombreux smartphones[52]
- Firmware de routeurs Cisco Systems[53, 54, 55]
- Firmware de routeurs Juniper Networks[54, 56]
- Firmware des disques durs Western Digital de la gamme de produits "My Cloud" (intégrant une solution de stockage dans le Cloud Computing)[57]

Notes et références

- **(en)** Cet article est partiellement ou en totalité issu de l'article de Wikipédia en anglais intitulé « Heartbleed (https://en.wikipedia.org/wiki/Heartbleed?oldid=603736300) » (voir la liste des auteurs (https://en.wikipedia.org/wiki/Heartbleed?action=history)).

1. **(en)** « Half a million widely trusted websites vulnerable to Heartbleed bug » (http://news.netcraft.com/archives/2014/04/08/half-a-million-widely-trusted-websites-vulnerable-to-heartbleed-bug.html) (Archivé (http://web.archive.org/web/*/http://news.netcraft.com/archives/2014/04/08/half-a-million-widely-trusted-websites-vulnerable-to-heartbleed-bug.html) • Wikiwix (http://archive.wikiwix.com/cache/?url=http://news.netcraft.com/archives/2014/04/08/half-a-million-widely-trusted-websites-vulnerable-to-heartbleed-bug.html) • Archive.is (http://archive.is/http://news.netcraft.com/archives/2014/04/08/half-a-million-widely-trusted-websites-vulnerable-to-heartbleed-bug.html) • Google (https://www.google.fr/search?q=cache:http://news.netcraft.com/archives/2014/04/08/half-a-million-widely-trusted-websites-vulnerable-to-heartbleed-bug.html) • Que faire ?), (consulté le 8 juin 2017), Netcraft, 8 avril 2014.
2. **(en)** « Man who introduced serious 'Heartbleed' security flaw denies he inserted it deliberately » (http://www.smh.com.au/it-pro/security-it/man-who-introduced-serious-heartbleed-security-flaw-denies-he-inserted-it-deliberately-20140410-zqta1.html), Sydney Morning Herald, 11 avril 2014.
3. « Meet the man who created the bug that almost broke the Internet », *Globe and Mail*, 11 avril 2014 (lire en ligne (https://www.theglobeandmail.com/news/national/meet-the-man-that-created-the-bug-that-almost-broke-the-internet/article17941003/)).
4. « #2658: [PATCH] Add TLS/DTLS Heartbeats » (http://rt.openssl.org/Ticket/Display.html?id=2658), OpenSSL, 2011.
5. **(en)** Codenomicon Ltd, « Heartbleed Bug » (http://heartbleed.com/), 8 avril 2014 (consulté le 8 avril 2014).
6. **(en)** Dan Goodin, « Critical crypto bug in OpenSSL opens two-thirds of the Web to eavesdropping » (https://arstechnica.com/security/2014/04/critical-crypto-bug-in-openssl-opens-two-thirds-of-the-web-to-eavesdropping/), *Ars Technica*, 8 avril 2014 (consulté le 8 avril 2014).
7. Site d'information sur le bug - heartbleed.com (http://heartbleed.com/), le 12 avril 2014.
8. Premier email d'information sur le bug (http://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=96db9023b881d7cd9f379b0c154650d6c108e9a3), 6 avril 2014, Site du référentiel d'OpenSSL.
9. « Que sait-on de « Heartbleed », l'inquiétante faille de sécurité sur Internet ? », *Le Monde*, 9 avril 2014 (lire en ligne (http://www.lemonde.fr/technologies/article/2014/04/09/une-enorme-faille-de-securite-dans-de-nombreux-sites-internet_4397995_651865.html)).
10. **(en)** « Group Backed by Google, Microsoft to Help Fund OpenSSL and Other Open Source Projects », *Threatpost | The first stop for security news*, 24 avril 2014 (lire en ligne (https://threatpost.com/group-backed-by-google-microsoft-to-help-fund-openssl-and-other-open-source-projects/105672/))
11. « Heartbleed : les géants du Net au secours des projets Open Source clés », *Silicon*, 24 avril 2014 (lire en ligne (http://www.silicon.fr/heartbleed-google-facebook-microsoft-financent-les-projets-open-source-cles-93972.html?utm_source=dlvr.it&utm_medium=twitter)).
12. Nicole Perlroth, « Companies Back Initiative to Support OpenSSL and Other Open-Source Projects » (https://bits.blogs.nytimes.com/2014/04/24/companies-back-initiative-to-support-openssl-and-other-open-source-projects/), *sur Bits Blog* (consulté le 16 mai 2017)
13. **(en)** Sean Gallagher, « Heartbleed vulnerability may have been exploited months before patch [Updated] », *Ars Technica*, 9 avril 2014 (lire en ligne (https://arstechnica.com/information-technology/2014/04/heartbleed-vulnerability-may-have-been-exploited-months-before-patch/))
14. **(en)** Peter Eckersley, « Wild at Heart: Were Intelligence Agencies Using Heartbleed in November 2013? », *Electronic Frontier Foundation*, 10 avril 2014 (lire en ligne (https://www.eff.org/deeplinks/2014/04/wild-heart-were-intelligence-agencies-using-heartbleed-november-2013))
15. **(en)** Jordan Robertson, « Millions of Android Devices Vulnerable to Heartbleed Bug » (https://www.bloomberg.com/news/2014-04-11/millions-of-android-devices-vulnerable-to-heartbleed-bug.html), *sur Bloomberg*, 12 avril 2014 (consulté le 13 avril 2014).
16. **(en)** Nick Sullivan, « Answering the Critical Question: Can You Get Private SSL Keys Using Heartbleed? » (http://blog.cloudflare.com/answering-the-critical-question-can-you-get-private-ssl-keys-using-heartbleed), *sur CloudFlare*, 11 avril 2014 (consulté le 12 avril 2014).
17. **(en)** « The Heartbleed Challenge » (https://www.cloudflarechallenge.com/heartbleed)(Archive (http://web.archive.org/web/*/https://www.cloudflarechallenge.com/heartbleed) • Wikiwix (http://archive.wikiwix.com/cache/?url=https://www.cloudflarechallenge.com/heartbleed) • Archive.is (http://archive.is/https://www.cloudflarechallenge.com/heartbleed) • Google (https://www.google.fr/search?q=cache:https://www.cloudflarechallenge.com/heartbleed) • Que faire ?), sur *CloudFlare*.
18. **(en)** Michael Riley, « NSA Said to Exploit Heartbleed Bug for Intelligence for Years » (https://www.bloomberg.com/news/2014-04-11/nsa-said-to-have-used-heartbleed-bug-exposing-consumers.html), sur *Bloomberg*, 12 avril 2014 (consulté le 12 avril 2014).
19. **(en)** ODNI Public Affairs Office, « IC on the Record » (http://icontherecord.tumblr.com/post/82416436703/statement-on-bloomberg-news-story-that-nsa-knew), sur *Office of the Director of National Intelligence, Tumblr*, 11 avril 2014 (consulté le 12 avril 2014).
20. « Heartbleed : attendez-vous à des lenteurs sur Internet » (http://www.lefigaro.fr/secteur/high-tech/2014/04/16/01007-20140416ARTFIG00044-reparer-heartbleed-va-ralentir-internet-dans-le-monde-entier.php), *sur Le Figaro*, 16 avril 2014 (consulté le 16 avril 2014).
21. « Heartbleed FAQ: Akamai Systems Patched », *Akamai Technologies*, 8 avril 2014 (lire en ligne (https://blogs.akamai.com/2014/04/heartbleed-faq-akamai-systems-patched.html)).
22. « AWS Services Updated to Address OpenSSL Vulnerability », *Amazon Web Services*, 8 avril 2014 (lire en ligne (https://aws.amazon.com/security/security-bulletins/aws-services-updated-to-address-openssl-vulnerability/)).
23. « Dear readers, please change your Ars account passwords ASAP », *Ars Technica*, 8 avril 2014 (lire en ligne (https://arstechnica.com/security/2014/04/dear-readers-please-change-your-ars-account-passwords-asap/)).
24. « All Heartbleed upgrades are now complete », *BitBucket Blog*, 9 avril 2014 (lire en ligne (http://blog.bitbucket.org/2014/04/09/all-heartbleed-upgrades-are-now-complete/)).
25. « Keeping Your BrandVerity Account Safe from the Heartbleed Bug », *BrandVerity Blog*, 9 avril 2014 (lire en ligne (http://blog.brandverity.com/2721/keeping-your-brandverity-account-safe-from-the-heartbleed-bug/)).
26. « Twitter / freenodestaff: we've had to restart a bunch... » (https://twitter.com/freenodestaff/status/453470038704795648), 8 avril 2014.
27. « Security: Heartbleed vulnerability », *GitHub*, 8 avril 2014 (lire en ligne (https://github.com/blog/1818-security-heartbleed-vulnerability)).
28. « IFTTT Says It Is 'No Longer Vulnerable' To Heartbleed », *LifeHacker*, 8 avril 2014 (lire en ligne (http://www.lifehacker.com.au/2014/04/ifttt-says-it-is-no-longer-vulnerable-to-heartbleed/)).
29. « Heartbleed bug and the Archive | Internet Archive Blogs » (https://blog.archive.org/2014/04/09/heartbleed-bug-and-the-archive/), Blog archive.org, 9 avril 2014 (consulté le 14 avril 2014).
30. « Twitter / KrisJelbring: If you logged in to any of » (https://twitter.com/KrisJelbring/status/453559871028613121), Twitter.com, 8 avril 2014 (consulté le 14 avril 2014).
31. Leo Kelion, « BBC News - Heartbleed hacks hit Mumsnet and Canada's tax agency » (http://www.bbc.co.uk/news/technology-27028101), BBC News, 14 avril 2014.
32. **(en)** « The widespread OpenSSL 'Heartbleed' bug is patched in PeerJ », *PeerJ*, 9 avril 2014 (lire en ligne (http://blog.peerj.com/post/82185230692/the-widespread-openssl-heartbleed-bug-is-patched-in)).
33. « Was Pinterest impacted by the Heartbleed issue? » (http://help.pinterest.com/en/articles/was-pinterest-impacted-heartbleed-issue), *Help Center*, Pinterest (consulté le 20 avril 2014).
34. « Heartbleed Defeated » (http://engineering.prezi.com/blog/2014/04/12/heartbleed/)(Archive (http://web.archive.org/web/*/http://engineering.prezi.com/blog/2014/04/12/heartbleed/) • Wikiwix (http://archive.wikiwix.com/cache/?url=http://engineering.prezi.com/blog/2014/04/12/heartbleed/) • Archive.is (http://archive.is/http://engineering.prezi.com/blog/2014/04/12/heartbleed/) • Google (https://www.google.fr/search?q=cache:http://engineering.prezi.com/blog/2014/04/12/heartbleed/) • Que faire ?) (consulté le 13 avril 2014).
35. Staff, « We recommend that you change your reddit password » (https://www.reddit.com/r/announcements/comments/231hl7/we_recommend_that_you_change_your_reddit_password), *Reddit*, 14 avril 2014 (consulté le 14 avril 2014).
36. « IMPORTANT ANNOUNCEMENTS FROM THE MAKERS OF CHILI » (http://forums.somethingawful.com/announcement.php?forumid=1) (consulté le 13 avril 2014).
37. Brendan Codey, « Security Update: We're going to sign out everyone today, here's why », *SoundCloud*, 9 avril 2014 (lire en ligne (http://blog.soundcloud.com/2014/04/09/heartbleed/)).
38. "ctsai", « SourceForge response to Heartbleed », *SourceForge*, 10 avril 2014 (lire en ligne (https://sourceforge.net/blog/sourceforge-response-to-heartbleed/)).
39. « Heartbleed », *SparkFun*, 9 avril 2014 (lire en ligne (https://www.sparkfun.com/news/1455)).
40. « Heartbleed », *Stripe (company)*, 9 avril 2014 (lire en ligne (https://stripe.com/blog/heartbleed)).
41. « Tumblr Staff-Urgent security update » (http://staff.tumblr.com/post/82113034874/urgent-security-update), 8 avril 2014 (consulté le 9 avril 2014).
42. Alex Hern, « Heartbleed: don't rush to update passwords, security experts warn », *The Guardian*, 9 avril 2014 (lire en ligne (https://www.theguardian.com/technology/2014/apr/09/heartbleed-dont-rush-to-update-passwords-security-experts-warn)).
43. Greg Grossmeier, « Wikimedia's response to the "Heartbleed" security vulnerability » (https://blog.wikimedia.org/2014/04/10/wikimedias-response-to-the-heartbleed-security-vulnerability/), *Wikimedia Foundation blog*, Wikimedia Foundation, 10 avril 2014 (consulté le 10 avril 2014).
44. « Wunderlist & the Heartbleed OpenSSL Vulnerability » (http://support.wunderlist.com/customer/portal/articles/1508382-sync-service-heartbleed---8th-of-april-2014), 10 avril 2014.
45. **(en)** IPCop, « IPCop 2.1.4 is released » (http://marc.info/?l=ipcop-announce&m=139697815506679), SourceForge electronic mailing lists, 8 avril 2014 (consulté le 11 avril 2014).
46. **(en)** italovignoli, « LibreOffice 4.2.3 is now available for download » (http://blog.documentfoundation.org/2014/04/10/libreoffice-4-2-3-is-now-available-for-download/) , sur *The Document Foundation*, 10 avril 2014 (consulté le 11 avril 2014).
47. « LogMeIn and OpenSSL », *LogMeIn*, 9 avril 2014 (lire en ligne (http://blog.logmein.com/products/openssl)).
48. « HP Servers Communication: OpenSSL "HeartBleed" Vulnerability » (http://h20566.www2.hp.com/portal/site/hpsc/template.PAGE/public/kb/docDisplay/?spf_p.tpst=kbDocDisplay&spf_p.prp_kbDocDisplay=wsrp-navigationalState%3Ddocid%253Demr_na-c04239413-1%257CdocLocale%253D%257CcalledBy%253D&javax.portlet.begCacheTok=com.vignette.cachetoken&javax.portlet.endCacheTok=com.vignette.cachetoken)(Archive (http://web.archive.org/web/*/http://h20566.www2.hp.com/portal/site/hpsc/template.PAGE/public/kb/docDisplay/?spf_p.tpst=kbDocDisplay&spf_p.prp_kbDocDisplay=wsrp-navigationalState%3Ddocid%253Demr_na-c04239413-1%257CdocLocale%253D%257CcalledBy%253D&javax.portlet.begCacheTok=com.vignette.cachetoken&javax.portlet.endCacheTok=com.vignette.cachetoken) • Wikiwix (http://archive.wikiwix.com/cache/?url=http://h20566.www2.hp.com/portal/site/hpsc/template.PAGE/public/kb/docDisplay/?spf_p.tpst=kbDocDisplay&spf_p.prp_kbDocDisplay=wsrp-navigationalState%3Ddocid%253Demr_na-c04239413-1%257CdocLocale%253D%257CcalledBy%253D&javax.portlet.begCacheTok=com.vignette.cachetoken&javax.portlet.endCacheTok=com.vignette.cachetoken) • Archive.is (http://archive.is/http://h20566.www2.hp.com/portal/site/hpsc/template.PAGE/public/kb/docDisplay/?spf_p.tpst=kbDocDisplay&spf_p.prp_kbDocDisplay=wsrp-navigationalState%3Ddocid%253Demr_na-c04239413-1%257CdocLocale%253D%257CcalledBy%253D&javax.portlet.begCacheTok=com.vignette.cachetoken&javax.portlet.endCacheTok=com.vignette.cachetoken) • Google (https://www.google.fr/search?q=cache:http://h20566.www2.hp.com/portal/site/hpsc/template.PAGE/public/kb/docDisplay/?spf_p.tpst=kbDocDisplay&spf_p.prp_kbDocDisplay=wsrp-navigationalState%3Ddocid%253Demr_na-c04239413-1%257CdocLocale%253D%257CcalledBy%253D&javax.portlet.begCacheTok=com.vignette.cachetoken&javax.portlet.endCacheTok=com.vignette.cachetoken) • Que faire ?), 18 avril 2014.
49. « McAfee Security Bulletin – OpenSSL Heartbleed vulnerability patched in McAfee products » (https://kc.mcafee.com/corporate/index?page=content&id=SB10071), sur *McAfee KnowledgeBase*, McAfee, 17 avril 2014.
50. « Response to OpenSSL security issue CVE-2014-0160/CVE-2014-0346 a.k.a: "Heartbleed" » (http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2076225), VMware, Inc (consulté le 17 avril 2014).
51. Paul Younger, « PC game services affected by Heartbleed and actions you need to take » (http://www.incgamers.com/2014/04/pc-game-services-affected-by-heartbleed-and-actions-you-need-to-take)(Archive (http://web.archive.org/web/*/http://www.incgamers.com/2014/04/pc-game-services-affected-by-heartbleed-and-actions-you-need-to-take) • Wikiwix (http://archive.wikiwix.com/cache/?url=http://www.incgamers.com/2014/04/pc-game-services-affected-by-heartbleed-and-actions-you-need-to-take) • Archive.is (http://archive.is/http://www.incgamers.com/2014/04/pc-game-services-affected-by-heartbleed-and-actions-you-need-to-take) • Google (https://www.google.fr/search?q=cache:http://www.incgamers.com/2014/04/pc-game-services-affected-by-heartbleed-and-actions-you-need-to-take) • Que faire ?), IncGamers, 11 avril 2014.
2. **(en)** « Heartbleed: Android 4.1.1 Jelly Bean could be seriously affected » (http://bgr.com/2014/04/16/heartbleed-android-4-1-1-jelly-bean), BGR Media, 16 avril 2014.
3. Alexis Kleinman, « The Heartbleed Bug Goes Even Deeper Than We Realized – Here's What You Should Do », *The Huffington Post*, 11 avril 2014 (lire en ligne (http://www.huffingtonpost.com/2014/04/11/heartbleed-bug_n_5132857.html)).

eartbleed-routers_n_5132306.html)).

4. **(en)** Danny Yadron, « Heartbleed Bug Found in Cisco Routers, Juniper Gear » (http://online.wsj.com/news/articles/SB10001424052702303873604579493963847851346?mg=reno64-wsj&url=http://online.wsj.com/article/SB10001424052702303873604579493963847851346.html)(Archive (http://web.archive.org/web/*/http://online.wsj.com/news/articles/SB10001424052702303873604579493963847851346?mg=reno64-wsj&url=http://online.wsj.com/article/SB10001424052702303873604579493963847851346.html) • Wikiwix (http://archive.wikiwix.com/cache/?url=http://online.wsj.com/news/articles/SB10001424052702303873604579493963847851346?mg=reno64-wsj&url=http://online.wsj.com/article/SB10001424052702303873604579493963847851346.html) • Archive.is (http://archive.is/http://online.wsj.com/news/articles/SB10001424052702303873604579493963847851346?mg=reno64-wsj&url=http://online.wsj.com/article/SB10001424052702303873604579493963847851346.html) • Google (https://www.google.fr/search?q=cache:http://online.wsj.com/news/articles/SB10001424052702303873604579493963847851346?mg=reno64-wsj&url=http://online.wsj.com/article/SB10001424052702303873604579493963847851346.html) • Que faire ?), Dow Jones & Company, Inc, 10 avril 2014.
5. **(en)** « Cisco Security Advisory: OpenSSL Heartbeat Extension Vulnerability in Multiple Cisco Products » (http://tools.cisco.com/security/center/mcontent/CiscoSecurityAdvisory/cisco-sa-20140409-heartbleed)(Archive (http://web.archive.org/web/*/http://tools.cisco.com/security/center/mcontent/CiscoSecurityAdvisory/cisco-sa-20140409-heartbleed) • Wikiwix (http://archive.wikiwix.com/cache/?url=http://tools.cisco.com/security/center/mcontent/CiscoSecurityAdvisory/cisco-sa-20140409-heartbleed) • Archive.is (http://archive.is/http://tools.cisco.com/security/center/mcontent/CiscoSecurityAdvisory/cisco-sa-20140409-heartbleed) • Google (https://www.google.fr/search?q=cache:http://tools.cisco.com/security/center/mcontent/CiscoSecurityAdvisory/cisco-sa-20140409-heartbleed) • Que faire ?), Cisco, 9 avril 2014.
6. **(en)** « 2014-04 Out of Cycle Security Bulletin: Multiple products affected by OpenSSL "Heartbleed" issue (CVE-2014-0160) » (http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10623), Juniper Networks, 14 avril 2014.
7. **(en)** « Heartbleed Bug Issue », *Western Digital*, 10 avril 2014 (lire en ligne (http://www.wdc.com/en/heartbleedupdate/)).

Annexes

Sur les autres projets Wikimedia :

Heartbleed, sur Wikinews

Articles connexes

- Trace numérique
- Vie privée et informatique

Liens externes

- Site d'information en anglais sur le bug (http://heartbleed.com/)
- Site d'information en français sur le bug (http://heartbleed.fr/)
- Pour tester la vulnérabilité d'un site (https://filippo.io/Heartbleed/)
- Article complet heartbleed sur commentcamarche.net (http://www.commentcamarche.net/faq/40044-faille-heartbleed-sites-web-concernes-et-conseils-pour-se-proteger)
