BULLETIN DE SECURITE DE LA SEMAINE DU 24 MARS 2014

Hautes Vulnérabilités

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source dôinformation & de correctif
adobe -- flash_player	Une vulnérabilité *Use-after-free* dans Adobe Flash Player 12.0.0.77 sur Windows permet à des attaquants distants d'exécuter du code arbitraire et de contourner un mécanisme de protection sandbox dôInternet Explorer via des vecteurs non spécifiés, comme l'a démontré VUPEN lors d'une compétition Pwn2Own pendant le CanSecWest 2014.	27/03/2014	10.0	CVE-2014-0506
adobe -- flash_player	Un débordement de tas dans Adobe Flash Player 12.0.0.77 permet à des attaquants distants d'exécuter du code arbitraire et de contourner un mécanisme de protection sandbox par des vecteurs non spécifiés, comme l'ont démontré Zeguang Zhao et Liang Chen lors d'une compétition Pwn2Own pendant le CanSecWest 2014.	27/03/2014	10.0	CVE-2014-0510
adobe -- acrobat_reader	Un débordement de tas dans Adobe Reader 11.0.06 permet à des attaquants distants d'exécuter du code arbitraire par des vecteurs non spécifiés, comme l'a démontré VUPEN lors d'une compétition Pwn2Own pendant le CanSecWest 2014.	27/03/2014	10.0	CVE-2014-0511
adobe -- acrobat_reader	Adobe Reader 11.0.06 permet à des attaquants de contourner un mécanisme de protection sandbox de PDF par des vecteurs non spécifiés, comme l'a démontré VUPEN lors d'une compétition Pwn2Own pendant le CanSecWest 2014.	27/03/2014	10.0	CVE-2014-0512
apache -- camel	Le composant XSLT des versions dôApache Camel 2.11.x à 2.11.4, 2.12.x à 2.12.3, et peut-être des versions antérieures, permet à des attaquants distants d'exécuter des méthodes Java arbitraires via un message façonné.	21/03/2014	7.5	CVE-2014-0003
apple -- safari	Une vulnérabilité non spécifiée dans Apple Safari 7.0.2 sur Mac OS X	26/03/2014	10.0	CVE-2014-1300

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source d'information & de correctif
	permet à des attaquants distants d'exécuter du code arbitraire avec les privilèges root via des vecteurs inconnus, comme l'a démontré Google lors d'une compétition de Pwn4Fun au CanSecWest 2014.			
apple -- safari	Un débordement de tas dans Apple Safari 7.0.2 permet à des attaquants distants d'exécuter du code arbitraire et de contourner un mécanisme de protection sandbox par des vecteurs non spécifiés, comme l'a démontré Liang Chen lors d'une compétition Pwn2Own pendant le CanSecWest 2014.	26/03/2014	10.0	CVE-2014-1303
b-e-soft -- artweaver_free	Un débordement de pile dans Artweaver Plus et free des versions antérieures à 3.1.5 permet à des attaquants distants d'exécuter du code arbitraire via un fichier d'image JPG façonné.	27/03/2014	9.3	CVE-2013-3481
cisco -- ios	Les versions Cisco IOS 15.3M à 15.3(3)M2 et IOS XE 3.10.xS à 3.10.2S permettent à des attaquants distants de causer un déni de service (rechargement de l'appareil) via les messages SIP façonnés, aka Bug ID CSCug45898.	27/03/2014	7.8	CVE-2014-2106
cisco -- ios	Cisco IOS 12.2 et 15.0 à 15.3, lorsqu'ils sont utilisés avec le Kailash FPGA versions antérieures à 2.6 sur les appareils RSP720-3C-10GE et RSP720-3CXL-10GE permettent à des attaquants distants de causer un déni de service (route switch processor outage) via les paquets IP façonnés, aka bug ID CSCug84789.	27/03/2014	7.1	CVE-2014-2107
cisco -- ios	Cisco IOS 12.2 et 15.0 à 15.3 et IOS XE 3.2 à 3.7 et antérieures à 3.7.5S et 3.8 à 3.10 et antérieures et 3.10.1S permettent à des attaquants distants de causer un déni de service (rechargement de l'appareil) via un paquet malformé IKEv2, aka Bug ID CSCui88426.	27/03/2014	7.8	CVE-2014-2108
cisco -- ios	Le module TCP d'entrée dans Cisco IOS 12.2 à 12.4 et 15.0 à 15.4, lorsque NAT est utilisé, permet à des attaquants distants de causer un déni de service (une consommation de mémoire ou un rechargement de l'appareil) via des paquets TCP façonnés, aka Bug IDs CSCuh33843 et CSCuj41494.	27/03/2014	7.8	CVE-2014-2109
cisco -- ios	Le module Application Layer Gateway (ALG) de Cisco IOS 12.2 à 12.4 et 15.0 à 15.4, quand NAT est utilisé, permet à des attaquants distants de causer un déni de service (rechargement de l'appareil) via des paquets DNS façonnés, alias Bug ID	27/03/2014	7.1	CVE-2014-2111

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source dûinformation & de correctif
	CSCue00996.			
cisco -- ios	La fonctionnalité VPN SSL (aka WebVPN) dans Cisco IOS 15.1 à 15.4 permet à des attaquants distants de causer un déni de service (consommation de mémoire) via des requêtes HTTP façonnées, aka Bug ID CSCuf51357.	27/03/2014	7.8	CVE-2014-2112
cisco -- ios	Cisco IOS 15.1 à 15.3 et IOS XE 3.3 à 3.5 à 3.5.2E, 3.7 à 3.7.5S; et 3.8, 3.9, et 3.10 à 3.10.2S permettent à des attaquants distants de causer un déni de service (consommation de mémoire I/O et rechargement de l'appareil) via un paquet IPv6 malformé, aka Bug ID CSCui59540.	27/03/2014	7.8	CVE-2014-2113
gplhost -- domain_technologie_control	La fonction *drawAdminTools_PackageInstaller* dans *shared/inc/forms/packager.php* de Domain Technologie Control (DTC) version antérieure à 0.32.11 permet à des attaquants distants d'exécuter des commandes arbitraires via des méta-caractères du shell dans le paramètre *dtcpkg_directory* lors dûne action de *do_install* dans dtc/.	21/03/2014	7.5	CVE-2011-5274
ibm -- datacap_taskmaster_capture	Un débordement de pile de Taskmaster Capture ActiveX control de IBM Datacap Taskmaster capture 8.0.1 et 8.1 antérieure à FP2, permet à des attaquants distants d'exécuter du code arbitraire par des vecteurs non précisées.	21/03/2014	9.3	CVE-2014-0879
ibm -- lotus_protector_for_mail_security	L'interface Web Admin UI dans IBM Lotus Protector pour Mail Security 2.8.x à 2.8.1-22905 permet à des utilisateurs authentifiés à distance de contourner les restrictions d'accès prévues et exécuter des commandes arbitraires via des vecteurs non précisées.	25/03/2014	7.1	CVE-2014-0886
ibm -- lotus_protector_for_mail_security	L'interface Web Admin UI dans IBM Lotus Protector de Mail Security 2.8.x à 2.8.1-22905 permet à des utilisateurs authentifiés à distance d'exécuter des commandes arbitraires avec les privilèges root via des vecteurs non précisées.	25/03/2014	7.1	CVE-2014-0887
ibm -- security_appscan	Le processus de mise à jour dans IBM Security AppScan Standard 7.9 à 8.8 ne nécessite pas de vérification de l'intégrité des fichiers téléchargés, ce qui permet à des attaquants distants d'exécuter du code arbitraire via un fichier façonné.	26/03/2014	7.6	CVE-2014-0904
kingsoft -- office_2012	Un débordement de pile de wpsio.dll dans Kingsoft WPS Office 2012 probablement la version 8.1.0.3238 permet à des attaquants distants d'exécuter du code arbitraire via une	24/03/2014	10.0	CVE-2012-4886

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source d'information & de correctif
	longue chaîne de caractères BSTR.			
linux -- linux_kernel	*net/netfilter/nf_conntrack_proto_dccp.c* dans le noyau Linux 3.13.6 utilise incorrectement un en-tête pointeur DCCP, ce qui permet aux attaquants distants de causer un déni de service (panne du système) ou éventuellement exécuter du code arbitraire via un paquet DCCP qui déclenche un appel au (1) dccp_new, (2) dccp_packet, ou (3) dccp_error fonction.	24/03/2014	10.0	CVE-2014-2523
maygion -- ip_camera_firmware	Un débordement de tampon dans les caméras IP MayGion dotées du firmware d'avant la date de 22/04/2013 (05.53) permet à des attaquants distants d'exécuter du code arbitraire via un long nom de fichier dans une requête GET.	25/03/2014	7.5	CVE-2013-1605
microsoft -- office	Microsoft Word 2003 SP3, 2007 SP3, 2010 SP1 et SP2, 2013, et 2013 RT; Word Viewer; Office Compatibility Pack SP3; Office pour Mac 2011; Word Automation Services sur SharePoint Server 2010 SP1 et SP2 et 2013; Office Web Apps 2010 SP1 et SP2; et Office Web Apps Serveur 2013 permettent à des attaquants distants d'exécuter du code arbitraire ou de causer un déni de service (corruption de mémoire) par l'intermédiaire des données RTF façonnées, comme exploitées sauvagement en Mars 2014.	25/03/2014	9.3	CVE-2014-1761
nuance -- pdf_reader	Un débordement de tas dans PDFCore8.dll de Nuance PDF Reader versions antérieures à 8.1 permet à des attaquants distants d'exécuter du code arbitraire viades valeurs modifiées du chemin d'accès de la table de police se trouvant dans un fichier RTF et concernant les entrées de la table de nommage..	27/03/2014	9.3	CVE-2013-0732
siemens -- simatic_s7_cpu-1211c	Le générateur de nombres aléatoires sur les appareils Siemens SIMATIC S7-1200 CPU PLC dotés du firmware antérieure à 4.0 n'a pas une entropie suffisante, ce qui rend plus facile à des attaquants distants de défaire les mécanismes de protection cryptographiques et de pirater les sessions via des vecteurs non précisés, une vulnérabilité différente de la référence CVE-2014 -2251.	24/03/2014	8.3	CVE-2014-2250
siemens -- simatic_s7_cpu-1211c	Les appareils Siemens SIMATIC S7-1200 CPU PLC munis du firmware antérieur à 4.0 permettent à des attaquants distants de causer un déni de service (transition vers le defect-mode) par l'intermédiaire de paquets HTTP façonnés, une vulnérabilité	24/03/2014	7.8	CVE-2014-2254

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source d'information & de correctif
	différente de la référence CVE-2014-2255.			
siemens -- simatic_s7_cpu-1211c	Les appareils Siemens SIMATIC S7-1200 CPU PLC munis du firmware antérieur à 4.0 permettent à des attaquants distants de causer un déni de service (transition vers le defect-mode) par l'intermédiaire paquets ISO-TSAP façonnés, une vulnérabilité différente de la référence CVE-2014-2257.	24/03/2014	7.8	CVE-2014-2256
siemens -- simatic_s7_cpu-1211c	Les appareils Siemens SIMATIC S7-1200 CPU PLC munis du firmware natérieur à 4.0 permettent des attaquants distants de causer un déni de service (transition vers le defect-mode) via des paquets HTTPS façonnés, une vulnérabilité différente de la référence CVE-2014-2259.	24/03/2014	7.8	CVE-2014-2258

Back to top

Moyennes Vulnérabilités

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source d'information & de correctif
barracudadrive -- barracudadrive	De nombreuses vulnérabilités Cross-Site Scripting (XSS) dans BarracudaDrive version antérieure à 6.7 permettent à des attaquants distants d'injecter des scripts web ou HTML arbitraires via le paramètre (1) sForumName ou (2) sDescription dans Forum/manage/ForumManager.lsp; le paramètre (3) sHhint, (4) sWord, ou (5) nId dans Forum/manage/hangman.lsp; (6) le paramètre utilisateur dans rtl/protected/admin/wizard/setuser.lsp; (7) le nom ou (8) le paramètre email dans feedback.lsp; (9) lname ou (10) le paramètre url dans private/manage/PageManager.lsp ; (11) le paramètre cmd dans fs; (12) newname, (13) description (14), firstname (15), lastname, ou (16) le paramètre id dans rtl/protected/mail/manage/list.lsp; ou (17) PATH_INFO dans fs/.	25/03/2014	4.3	CVE-2014-2526
cacti -- cacti	Une vulnérabilité Cross-site scripting (XSS) dans Cacti 0.8.7g permet à des attaquants distants d'injecter des scripts web ou HTML arbitraires par des vecteurs non précisées.	27/03/2014	4.3	CVE-2014-2326

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source dôinformation & de correctif
christos_zoulas -- file	Lôexpression régulière BEGIN dans le détecteur de script dôawk placée dans *magic/Magdir/commands* dans le fichier version antérieure à 5.15 utilise plusieurs astérisques avec des répétitions illimitées, ce qui permet à des attaquants dépendant du contexte de causer un déni de service (consommation de CPU) via un fichier ASCII façonné qui déclenche une grande quantité de retour en arrière, comme prouvé par un fichier avec de nombreux caractères de ligne nouvelle.	24/03/2014	5.0	CVE-2013-7345
cisco -- prime_security_manager	De multiples vulnérabilités Cross-Site Scripting (XSS) dans les documents HTML qui sont liés au tableau de bord de Cisco Prime Security Manager (aka PRSM) 9.2 (.1-2) et précédents permettent à des attaquants distants d'injecter des scripts web ou HTML arbitraires via des paramètres non spécifiés, alias Bug ID CSCun50687.	27/03/2014	4.3	CVE-2014-2118
dell -- sonicwall_network_security_appliance_2400	Une vulnérabilité Cross-site scripting (XSS) dans le service Dashboard Backend (stats/dashboard.jsp) dans SonicWall Network Security Appliance (NSA) 2400 permet à des attaquants distants d'injecter des scripts web ou HTML arbitraires via le paramètre sn.	24/03/2014	4.3	CVE-2014-2589
emc -- rsa_bsafe	Le serveur dans EMC RSA BSAFE Micro Edition Suite (MES) 4.0.x à 4.0.5 ne traite pas correctement les chaînes de certificat, ce qui permet à des attaquants distants afin de causer un déni de service (panne de daemon) par des vecteurs non précisées.	25/03/2014	5.0	CVE-2014-0628
flowplayer ï flowplayer_flash	De multiples vulnérabilités Cross-Site Scripting (XSS) dans Flowplayer Flash version antérieure à 3.2.17, tel qu'il est utilisé dans Moodle version 2.3.11, 2.4.x à 2.4.9, 2.5.x à 2.5.5, 2.6.x à 2.6.2, permettent à des attaquants distants d'injecter des scripts web ou HTML arbitraires par (1) la fourniture d'un playerId façonné ou (2) le référencement à un domaine externe, un problème lié à la référence	24/03/2014	4.3	CVE-2013-7341

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source d'information & de correctif
	CVE-2013-7342.			
flowplayer -- flowplayer_html5	Une vulnérabilité Cross-site scripting (XSS) dans flowplayer.swf dans la fonction Flash fallback dans Flowplayer HTML5 5.4.1 permet à des attaquants distants d'injecter des scripts web ou HTML arbitraires via le paramètre de rappel, un problème lié à la référence CVE-2013-7341.	24/03/2014	4.3	CVE-2013-7342
flowplayer -- flowplayer_html5	Une vulnérabilité Cross-site scripting (XSS) dans flowplayer.swf dans la fonction Flash fallback dans Flowplayer HTML5 5.4.3 permet à des attaquants distants d'injecter des scripts web ou HTML arbitraires en utilisant l'encodage d'URL dans le nom du paramètre de rappel. NOTE: Cette vulnérabilité existe en raison d'un correctif incomplet pour la référence CVE-2013-7342.	24/03/2014	4.3	CVE-2013-7343
gplhost -- domain_technologie_ control	Une vulnérabilité d'injection SQL dans Domain Technologie Control (DTC) version avant 0.34.1 permet les utilisateurs authentifiés à distance d'exécuter des commandes arbitraires SQL via le paramètre addrlink dans shared/inc/forms/domain_info.php. REMARQUE: CVE-2011-3197 a été scindée en raison des découvertes faites par différents chercheurs. CVE-2011-5272 a été attribué pour le paramètre vps_note au vecteur dtcadmin/logPushlet.php.	21/03/2014	6.5	CVE-2011-3197
gplhost -- domain_technologie_ control	Une vulnérabilité d'injection SQL dans Domain Technologie Control (DTC) version antérieure à 0.34.1 permet à des utilisateurs authentifiés à distance d'exécuter des commandes arbitraires SQL via le paramètre vps_note dans dtcadmin/logPushlet.php. REMARQUE: ce problème faisait partie à l'origine de la référence CVE-2011-3197, mais le numéro d'identification a été divisé en raison de différentes recherches	21/03/2014	6.5	CVE-2011-5272
ibm -- infosphere_biginsights	La vulnérabilité « Open redirect » de Web Application Enterprise Console dans IBM InfoSphere BigInsights 1.1 et 2.x à 2.1 FP2 permet aux	26/03/2014	4.9	CVE-2013-3997

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source dôinformation & de correctif
	utilisateurs authentifiés à distance de rediriger les utilisateurs vers des sites Web arbitraires et conduire des attaques de phishing via des vecteurs non précisées.			
ibm -- websphere_mq_internet_pass_thru	Le processus dôécoute des command sur ports dans IBM WebSphere MQ Internet Pass-Thru (MQIPT) 2.x à 2.1.0.1 permet à des attaquants distants de causer un déni de service (à distance administration panne) par des vecteurs non précisées.	21/03/2014	5.0	CVE-2013-5401
ibm -- cognos_express	La vulnérabilité Cross-site request forgery (CSRF) dans IBM Cognos Express 9.0 antérieure à IFIX 2, 9.5 , antérieure à IFIX 2, 10.1 antérieure à IFIX 2, et 10.2.1 antérieure à FP1 permet à des attaquants distants afin de détourner l'authentification des utilisateurs arbitraires.	25/03/2014	6.8	CVE-2013-5443
ibm -- cognos_express	Le serveur dans IBM Cognos Express 9.0 avant IFIX 2, 9.5 avant IFIX 2, 10.1 avant IFIX 2, et 10.2.1 avant FP1 permet à des attaquants distants de lire les informations d'identification cryptées par des vecteurs non précisées.	25/03/2014	5.0	CVE-2013-5444
ibm -- cognos_express	IBM Cognos Express 9.0 avant IFIX 2, 9.5 avant IFIX 2, 10.1 avant IFIX 2, et 10.2.1 avant FP1 permet aux utilisateurs locaux d'obtenir des informations sensibles en clair en s'appuyant sur la connaissance d'une clé de décryptage statique.	25/03/2014	5.0	CVE-2013-5445
ibm -- rational_clearcase	Plusieurs débordements de tampon dans IBM Rational ClearCase 7.x avant 7.1.2.13, 8.0.0.10 8.0.0.x avant, et 8.0.1.x avant 8.0.1.3 permettent aux utilisateurs authentifiés à distance dôobtenir un accès privilégié par des vecteurs non précisées.	21/03/2014	6.5	CVE-2014-0829
ibm -- lotus_protector_for_mail_security	La vulnérabilité Cross-site request forgery (CSRF) dans l'interface Web dôAdministration dans IBM Lotus Protector pour Mail Security 2.8.x à 2.8.1-22905 permet aux utilisateurs authentifiés à distance de détourner l'authentification de victimes non	25/03/2014	6.8	CVE-2014-0885

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source d'information & de correctif
	précisés par des vecteurs inconnus.			
icinga -- icinga	De multiples off-by-one erreurs dans Icinga, probablement la version 1.10.2 et versions antérieures, permettent à des attaquants distants de causer un déni de service (crash) par des vecteurs non précisées à la fonction (1) display_nav_table, (2) print_export_link, (3) page_num_selector, ou (4) page_limit_selector dans cgi/cgiutils.c ou la fonction (5) status_page_num_selector dans cgi/status.c, ce qui déclenche un débordement de mémoire tampon en fonction.	25/03/2014	5.0	CVE-2014-2386
ithoughts -- ithoughtshd	L'application iThoughtsHD 4.19 pour iOS sur les appareils iPad, lorsque la fonction de transfert WiFi Transfer est utilisée, permet à des attaquants distants de transférer des fichiers arbitraires en plaçant une séquence %00 après une extension dangereuse, comme l'a démontré un fichier html%00.txt.	26/03/2014	4.3	CVE-2014-1827
ithoughts -- ithoughtshd	Le serveur Web iThoughts dans l'application iThoughtsHD 4.19 pour iOS sur les appareils iPad permet à des attaquants distants afin de causer un déni de service (consommation du disque) en transférant un fichier de grande taille.	26/03/2014	4.3	CVE-2014-1828
joshua_peek -- rack-ssl	Une vulnérabilité Cross-site scripting (XSS) dans lib/rack/ssl.rb dans rack-ssl gem version avant 1.4.0 pour Ruby permet à des attaquants distants d'injecter des scripts web ou HTML arbitraires via un URI, qui pourrait ne pas être correctement pris en charge par adaptateurs tiers tels que JRuby-Rack.	25/03/2014	4.3	CVE-2014-2538
linux -- linux_kernel	La fonction rds_ib_laddr_check dans net/rds/ib.c dans le noyau Linux version avant 3.12.8 permet aux utilisateurs locaux afin de causer un déni de service (déréférencement NULL pointeur et plantage du système) ou éventuellement avoir d'autres effets non spécifiés via un appel système de liaison pour un	24/03/2014	4.7	CVE-2013-7339

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source d'information & de correctif
	socket RDS sur un système qui manque de transports RDS.			
maygion -- ip_camera_firmware	Une vulnérabilité « traversée de répertoire » dans les caméras IP MayGion dotées du micrologiciel d'avant le 22/04/2013 (05.53) permet à des attaquants distants de lire des fichiers arbitraires via des .. (point point) dans l'URI par défaut.	25/03/2014	5.0	CVE-2013-1604
mcafee -- cloud_single_sign_on	Une vulnérabilité Cross-site scripting (XSS) dans le formulaire de vérification de connexion dans McAfee Cloud Single Sign On (SSO) permet à des attaquants distants d'injecter des scripts web ou HTML arbitraires via un mot de passe falsifié.	24/03/2014	4.3	CVE-2014-2586
mcafee -- asset_manager	Une vulnérabilité d'injection SQL dans *jsp/reports/ReportsAudit.jsp* dans McAfee Asset Manager 6.6 permet aux utilisateurs authentifiés à distance d'exécuter des commandes arbitraires SQL via le nom d'utilisateur d'un rapport d'audit (paramètre utilisateur aka).	24/03/2014	6.5	CVE-2014-2587
mcafee -- asset_manager	Une vulnérabilité de traversée de répertoire dans *servlet/downloadReport* dans McAfee Asset Manager 6.6 permet aux utilisateurs authentifiés à distance de lire des fichiers arbitraires via des .. (point point) dans le paramètre reportFileName.	24/03/2014	4.0	CVE-2014-2588
moodle -- moodle	Le fichier *mod/chat/chat_ajax.php* dans Moodle des versions 2.3.11, 2.4.x à 2.4.9, 2.5.x à 2.5.5, 2.6.x à 2.6.2 ne vérifie pas correctement la fonctionnalité *mod/chat:chat* pendant les sessions de chat, ce qui permet à des utilisateurs authentifiés à distance, dans des circonstances opportunistes, de contourner les restrictions d'accès prévues en restant dans une session de chat après une suppression d'un fonctionnement en mode intra-session par un administrateur.	24/03/2014	4.9	CVE-2014-0122
moodle -- moodle	Le sous-système wiki dans Moodle 2.3.11, 2.4.x à 2.4.9, 2.5.x à 2.5.5, 2.6.x à 2.6.2 ne restreint pas	24/03/2014	4.9	CVE-2014-0123

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source dôinformation & de correctif
	correctement lôaccès à (1) view (Vue) et (2) edit (Edition), ce qui permet aux utilisateurs authentifiés à distance dôeffectuer des opérations de wiki en s'appuyant sur le rôle de l'élève et en utilisant le bloc Activité récente pour atteindre le wiki individuel d'un étudiant quelconque.			
moodle -- moodle	Les implémentations *identity-reporting* dans *mod/forum/renderer.php* et *mod/quiz/override_form.php* dans Moodle 2.3.11, 2.4.x à 2.4.9, 2.5.x à 2.5.5 et 2.6.x à 2.6.2 ne restreignent pas correctement l'affichage des adresses e-mail, ce qui permet aux utilisateurs authentifiés à distance dôobtenir des informations sensibles à travers les modules (1) Forum ou (2) Quiz.	24/03/2014	4.0	CVE-2014-0124
moodle -- moodle	Le fichier *repository/alfresco/lib.php* dans Moodle 2.3.11, 2.4.x à 2.4.9, 2.5.x à 2.5.5, 2.6.x à 2.6.2 place une clé de session dans une URL, ce qui permet à des attaquants distants de contourner les restrictions prévues pour le fichier du dépôt Alfresco en se faisant passer pour le propriétaire d'un fichier.	24/03/2014	5.8	CVE-2014-0125
moodle -- moodle	Une vulnérabilité Cross-site request forgery (CSRF) dans *enrol/imsenterprise/importnow.php* dans Moodle 2.3.11, 2.4.x à 2.4.9, 2.5.x à 2.5.5 et 2.6.x à 2.6.2 permet à des attaquants distants de détourner l'authentification des administrateurs pour les demandes qui importent un fichier IMS Enterprise.	24/03/2014	6.8	CVE-2014-0126
moodle -- moodle	Lôimplémentation time-validation dans (1) *mod/feedback/complete.php* et (2) *mod/feedback/complete_guest.php* dans Moodle 2.3.11, 2.4.x à 2.4.9, 2.5.x à 2.5.5, et 2.6.x à2.6.2 permet aux utilisateurs authentifiés à distance de contourner les restrictions prévues en démarrant une activité de Feedback par le choix dôun temps non disponible.	24/03/2014	4.9	CVE-2014-0127

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source dôinformation & de correctif
moodle -- moodle	badges/mybadges.php dans Moodle 2.5.x à 2.5.5 et 2.6.x à 2.6.2 ne suit pas correctement l'utilisateur à qui un badge a été attribué, ce qui permet à des utilisateurs authentifiés à distance de modifier la visibilité d'un badge arbitraire via des vecteurs indéterminés.	24/03/2014	4.0	CVE-2014-0129
moodle -- moodle	mod/assign/externallib.php dans Moodle 2.6.x à 2.6.2 ne gère pas correctement lôaffectation des paramètres web-service, ce qui pourrait permettre aux utilisateurs authentifiés à distance de modifier des métadonnées de qualité par des vecteurs non précisées.	24/03/2014	4.0	CVE-2014-2572
mozilla -- network_security_ services	La fonction de *cert_TestHostName* dans *lib/certdb/certdb.c* dans lôimplémentation de la vérification du certificat dans Mozilla Network Security Services (NSS) avant 3.16 accepte un caractère générique qui est incorporé dans U-label d'un nom de domaine internationalisé, ce qui pourrait permettre à des attaquants « man-in-the-middle » dôusurper des SSL serveurs au moyen dôun certificat falsifié.	25/03/2014	4.3	CVE-2014-1492
net-snmp -- net-snmp	L'implémentation Linux d'ICMP-MIB dans Net-SNMP 5.5 à 5.5.2.1, 5.6.x à 5.6.2.1 et 5.7.x à 5.7.2.1 ne valide pas correctement les entrées, ce qui permet à des attaquants distants de causer un déni de service par des vecteurs non précisées.	24/03/2014	5.0	CVE-2014-2284
openbsd -- openssh	La fonction verify_host_key dans sshconnect.c dans le client dans OpenSSH 6.6 et les versions antérieures permet à des serveurs distants dôannuler le contrôle de SSHFP DNS RR en présentant un HostCertificate inacceptable.	27/03/2014	5.8	CVE-2014-2653
opensolution -- quick_ cart	Une vulnérabilité Cross-site scripting (XSS) dans Open Solution 5.0 Quick.Cms et Quick.Cart 6.0, probablement téléchargé avant le 19 Décembre 2012, permet à des attaquants distants d'injecter des scripts web ou HTML arbitraires via le PATH_INFO dans admin.php.	24/03/2014	4.3	CVE-2012-6430

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source dôinformation & de correctif
	NOTE: ce pourrait être un duplicata de la référence CVE-2008-4140.			
openssl -- openssl	La mise en î uvre de l'échelle Montgomery dans OpenSSL 1.0.0l ne garantit pas que certaines opérations swap ont un comportement constant dans le temps, ce qui rend plus facile pour les utilisateurs locaux dôobtenir des nonces ECDSA via une attaque par canal auxiliaire FLUSH+RELOAD.	25/03/2014	4.3	CVE-2014-0076
owncloud -- owncloud	Une vulnérabilité non spécifiée dans *core/ajax/translations.php* dans ownCloud versions antérieures à 4.0.12 et 4.5.x à 4.5.6 permet à des utilisateurs authentifiés à distance d'exécuter du code PHP arbitraire via des vecteurs inconnus. NOTE: cette entrée a été scindée en raison des différentes versions affectées. Le problème core/settings.php est couvert par la référence CVE-2013-7344.	24/03/2014	6.5	CVE-2013-0303
owncloud -- owncloud	Une vulnérabilité non spécifiée dans core/settings.php dans ownCloud avant 4.0.12 et 4.5.x à 4.5.6 permet à des utilisateurs authentifiés à distance d'exécuter du code PHP arbitraire via des vecteurs inconnus. REMARQUE: ce problème a été découpé de la référence CVE-2013-0303 en raison de différentes versions affectées.	24/03/2014	6.5	CVE-2013-7344
owncloud -- owncloud	Plusieurs cross-site scripting (XSS) dans ownCloud avant 6.0.2 permettent à des attaquants distants d'injecter des scripts web ou HTML arbitraires par des vecteurs non précisées.	24/03/2014	4.3	CVE-2014-2057
owncloud -- owncloud	ownCloud avant 5.0.15 et 6.x à 6.0.2, lorsque l'application file_external est activée, permet à des utilisateurs authentifiés à distance de monter le système de fichiers local dans le ownCloud de l'utilisateur via la configuration de montage.	24/03/2014	4.9	CVE-2014-2585
oxid-esales -- eshop	De multiples Cross-Site Scripting (XSS) dans OXID eShop Professional and Community Edition 4.6.8 et les	25/03/2014	4.3	CVE-2014-2016

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source d'information & de correctif
	versions antérieures, 4.7.x à 4.7.11 et 4.8.x à 4.8.4, et Enterprise Edition 4.6.8 et les versions antérieures, 5.0.x avant 5.0.11 et 5.1.x à 5.1.4, permettent à des attaquants distants d'injecter des scripts web ou HTML arbitraires via le paramètre searchtag dans la fonction getTag dans (1) application/controllers/details.php ou dans (2) application/controllers/tag.php.			
php -- php	La fonction gdImageCreateFromXpm dans gdxpm.c dans libgd, telle qu'utilisée dans PHP 5.4.26 et antérieures, permet à des attaquants distants de causer un déni de service (déréférencement NULL pointeur et plantage de l'application) via une table de couleur falsifiée dans un fichier XPM.	21/03/2014	4.3	CVE-2014-2497
redhat -- enterprise_linux	La fonction get_rx_bufs dans drivers/vhost/net.c dans le sous-système vhost-net dans le paquet du noyau Linux avant 2.6.32-431.11.2 sur Red Hat Enterprise Linux (RHEL) 6 ne gère pas correctement les erreurs de vhost_get_vq_desc, ce qui permet aux utilisateurs des OS clients de causer un déni de service (crash du système d'exploitation hôte) par des vecteurs non précisées.	26/03/2014	5.5	CVE-2014-0055
rsa -- authentication_manager	Une vulnérabilité Cross-site scripting (XSS) dans la console Self-Service dans EMC RSA Authentication Manager 7.1 avant SP4 P32 permet à des attaquants distants d'injecter des scripts web ou HTML arbitraires via des vecteurs non spécifiés, liés à un problème "cross frame script".	27/03/2014	4.3	CVE-2014-0623
siemens -- simatic_s7_ cpu-1211c	Les appareils Siemens SIMATIC S7-1200 CPU PLC avec firmware avant 4.0 permettent à des attaquants distants de causer un déni de service (transition defect-mode) par des paquets de PROFINET falsifiés, une vulnérabilité différente de la référence CVE-2014-2253.	24/03/2014	6.1	CVE-2014-2252
stunnel -- stunnel	stunnel avant 5.00, lors de l'utilisation de « fork threading », ne met pas correctement à jour l'état de pseudo-	24/03/2014	4.3	CVE-2014-0016

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source dôinformation & de correctif
	générateur de nombres aléatoires (PRNG) dôOpenSSL, ce qui entraîne les « processus » enfants ultérieurs avec le même ID processus à utiliser le même pool d'entropie et permet à des attaquants distants d'obtenir des clés privées pour les certificats EC (ECDSA) ou DSA.			
symphony-cms -- symphony_cms	Une vulnérabilité d'injection SQL dans Symphony CMS avant 2.3.2 permet aux utilisateurs authentifiés à distance d'exécuter des commandes SQL arbitraires via le paramètre de tri dans system/authors/. NOTE: ce peut être exploité en utilisant CSRF pour permettre à des attaquants distants non authentifiés d'exécuter des commandes arbitraires SQL.	27/03/2014	6.5	CVE-2013-2559
symphony-cms -- symphony_cms	Une vulnérabilité Cross-site request forgery (CSRF) dans Symphony CMS avant 2.3.2 permet à des attaquants distants de détourner l'authentification des administrateurs pour les requêtes qui effectuent des attaques par injection SQL via le paramètre de tri dans system/authors/, liés à la référence CVE-2013-2559.	27/03/2014	6.8	CVE-2013-7346
theforeman -- foreman	Une vulnérabilité Cross-site scripting (XSS) dans app/views/common/500.html.erb dans Foreman 1.4.x à 1.4.2 permet à des utilisateurs authentifiés à distance dôinjecter un script web ou HTML arbitraires via le nom du signet lors de l'ajout d'un signet.	27/03/2014	4.3	CVE-2014-0089
trojita_project -- trojita	La fonction OpenConnectionTask :: handleStateHelper dans Imap/Tasks/OpenConnectionTask.cpp dans Trojita avant 0.4.1 permet à des attaquants man-in-the-middle de déclencher l'utilisation de cleartext pour l'enregistrement d'un message dans un dossier (1) envoyé (sent) ou (2) brouillon (draft) via une réponse PREAUTH qui empêche une utilisation ultérieure de la commande STARTTLS.	21/03/2014	4.3	CVE-2014-2567
videolan -- vlc_media_player	VideoLAN VLC Media Player avant 2.0.7 permet à des attaquants distants afin de causer un déni de service	21/03/2014	4.3	CVE-2013-7340

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source dâinformation & de correctif
	(consommation de mémoire) via un fichier de playlist falsifié.			
virtualaccess -- gw6110a	L'interface Web dans Virtual Access GW6110A routers avec le logiciel 9.00 à 9.09.27, 9.50 à 9.50.21 et 10.00 à 10.00.21, permet à des utilisateurs authentifiés à distance dâobtenir des privilèges via une variable JavaScript modifiée.	25/03/2014	4.9	CVE-2014-0343
wysija_newsletters_project -- wysija_newsletters	Plusieurs vulnérabilités d'injection SQL dans le plugin Wysija Newsletters avant 2.2.1 pour WordPress permettent aux administrateurs à distance authentifiés d'exécuter des commandes arbitraires SQL via le paramètre (1) recherche ou (2) orderby dans wp-admin/admin.php. NOTE: cela peut être exploité en utilisant CSRF pour permettre à des attaquants distants non authentifiés d'exécuter des commandes arbitraires SQL.	24/03/2014	6.5	CVE-2013-1408

Back to top

Faibles Vulnérabilités

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source dâinformation & de correctif
extplorer -- extplorer	De multiples Cross-Site Scripting (XSS) dans eXtplorer 2.1.3, lorsqu'il est utilisé comme composant pour Joomla!, permettent à des attaquants distants d'injecter des scripts web ou HTML arbitraires via le PATH_INFO dans (1) application.js.php placé dans scripts/ ou (2) admin.php, (3) copy_move.php, (4) functions.php, (5) header.php, ou (6) upload.php placé dans include/.	25/03/2014	2.6	CVE-2013-5951
gplhost -- domain_technologie_control	Le script de configuration dans le Domain Technologie de contrôle (DTC) avant 0.34.1 utilise les autorisations lisible pour tous pour /etc/apache2/apache2.conf, ce qui permet aux utilisateurs locaux d'obtenir le mot de passe MySQL dtcdaemons par la lecture du fichier.	21/03/2014	2.1	CVE-2011-3196
gplhost -- domain_technologie_control	De multiples Cross-Site Scripting (XSS) dans Domain Technologie de contrôle (DTC) avant 0.34.1 permettent aux utilisateurs authentifiés à distance dâinjecter des scripts web ou HTML arbitraires via le	21/03/2014	3.5	CVE-2011-3199

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source dãinformation & de correctif
	(1) le corps du message d'un ticket de support ou des vecteurs non spécifiées dans le (2) DNS et (3) dans le formulaire MX, tel que démontré par le champ "Domain root TXT record:"			
ibm -- data_protection	La (1) composante Data Protection for Exchange 6.1 à6.1.3.4 et 6.3 à 6.3.1 dans IBM Tivoli Storage Manager pour Mail et la composante (2) FlashCopy Manager pour Exchange 2.2 et 3.1 à 3.1.1 dans IBM Tivoli Storage FlashCopy Manager ne contraignent pas correctement le contenu de la boîte aux lettres pendant certaines opérations PST de restauration, qui permet aux utilisateurs authentifiés à distance de lire l'e-mail personnel d'autres utilisateurs dans des circonstances opportunistes par le lancement d'un client e-mail après qu'un administrateur ait effectué une restauration de nombreuses boîtes aux lettres.	26/03/2014	2.1	CVE-2013-3976
ibm -- infosphere_biginsights	Une vulnérabilité d'injection CRLF dans Web Application Enterprise Console dans IBM InfoSphere BigInsights 1.1 et 2.x à 2.1 FP2 permet aux utilisateurs authentifiés à distance dãinjecter des entêtes HTTP arbitraires et mener une attaque par fractionnement de réponse HTTP via des vecteurs non précisées.	26/03/2014	3.5	CVE-2013-3998
ibm -- quickfile	Une vulnérabilité Cross-site scripting (XSS) dans IBM QuickFile 1.0.0.0 avant iFix 4 et 1.1.0.1, avant iFix 3 permet à distance des utilisateurs authentifiés à injecter un script web ou HTML arbitraires via une URL conçue.	21/03/2014	3.5	CVE-2013-6729
ibm -- netezza_performance_portal	Les fichiers (1) ssl.conf et (2) httpd.conf dans la composante Serveur HTTP Apache dans IBM Netezza Performance Portal 2.0 à 2.0.0.4 ont des valeurs SSLCipherSuite faibles, ce qui rend plus facile pour les attaquants distants de vaincre les mécanismes cryptographiques de protection via une attaque par force brute.	26/03/2014	3.5	CVE-2014-0848
ibm -- lotus_protector_for_mail_security	Une vulnérabilité Cross-site scripting (XSS) dans l'interface Web Admin dans IBM Lotus Protector pour Mail Security 2.8.x à 2.8.1-22905 permet aux utilisateurs authentifiés à distance pour injecter des scripts web ou HTML arbitraires par des vecteurs non précisées.	25/03/2014	3.5	CVE-2014-0884
ithoughts -- ithoughtshd	Une vulnérabilité Cross-site scripting (XSS) dans l'application de iThoughtsHD 4.19 pour iOS sur les appareils iPad, lorsque la fonction de transfert WiFi est utilisée, permet à des attaquants distants d'injecter des scripts web ou HTML arbitraires via un nom de carte conçu.	26/03/2014	2.6	CVE-2014-1826
linux -- linux_kernel	Une vulnérabilité Use-after-free dans la fonction skb_segment placé dans net/core/skbuff.c dans le noyau Linux jusquãà 3.13.6 permet aux attaquants	24/03/2014	2.9	CVE-2014-0131

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source dâinformation & de correctif
	d'obtenir des informations sensibles de la mémoire du noyau en tirant parti de l'absence d'une certaine opération orphelines.			
linux -- linux_kernel	Une vulnérabilité Use-after-free dans la fonction nfqnl_zcopy placé dans net/netfilter/nfnetlink_queue_core.c dans le noyau Linux jusquâà 3.13.6 permet aux attaquants d'obtenir des informations sensibles de la mémoire du noyau en tirant parti de l'absence d'une certaine opération orpheline. NOTE: le code affecté a été transféré à la fonction skb_zerocopy en net/core/skbuff.c avant que la vulnérabilité soit annoncée.	24/03/2014	2.9	CVE-2014-2568
moodle -- moodle	Une vulnérabilité Cross-site scripting (XSS) dans la fonction quiz_question_tostring dans mod/quiz/editlib.php dans Moodle jusquâà 2.3.11, 2.4.x à 2.4.9, 2.5.x à 2.5.5, 2.6.x à 2.6.2 permet aux utilisateurs authentifiés à distance dâinjecter des scripts web ou HTML arbitraires via un quiz.	24/03/2014	3.5	CVE-2014-2571
mozilla -- firefox	Mozilla Firefox avant 28.0.1 sur Android traite un fichier URL en copiant un fichier local sur la carte SD, ce qui permet aux pirates d'obtenir des informations sensibles à partir du répertoire de profil Firefox via une application conçue.	25/03/2014	1.9	CVE-2014-1515
openstack -- compute	Le pilote VMWare dans OpenStack Compute (Nova) 2013.2 à 2013.2.2 ne met pas correctement les machines virtuelles en mode secours, ce qui permet aux utilisateurs distants autorisés de contourner la limite de quota et provoquer un déni de service (consommation des ressources) en demandant la VM se mettre en mode secours puis de supprimer l'image.	25/03/2014	2.3	CVE-2014-2573

Back to top