Bulletin hebdomadaire des vulnérabilités n°BV14-04

Date de publication : 24/04/2014

Le Centre National de Cybersécurité (CIRT-BF) publie à la date ci-dessus mentionnée son Bulletin hebdomadaire des vulnérabilités. Ce bulletin est un listing des vulnérabilités enregistrées dans les bases de données de CVE au cours de la période indiquée. Le bulletin comprend trois types de vulnérabilités selon leur degré de sévérité.

Ainsi on distingue :

- Les **Vulnérabilités critiques** : il sâagit de celles ayant un score CVSS compris entre 7.0 et 10
- Les **Vulnérabilités majeures** : il sâagit de celles ayant un score CVSS compris entre 4.0 et 6.9
- Les **Vulnérabilités mineures** : il sâagit de celles ayant un score CVSS compris entre 0.0 et 3.9

Les vulnérabilités sont résumées dans des tableaux qui comportent 5 colonnes et fournissant les informations suivantes :

- Le nom de l**âéditeur principal et le nom du produit** vulnérable (colonne 1)
- Une **description** synthétique de la vulnérabilité (colonne 2)
- La **date de publication** de la vulnérabilité (colonne 3)
- Le **score CVSS** (Common Vulnerability Scoring System) de la vulnérabilité (colonne 4)
- La **référence CVE** de la vulnérabilité permettant dâavoir des informations complémentaires et de correctifs (colonne 5)

Le Bulletin hebdomadaire des vulnérabilités publié par CIRT-BF est une traduction-maison des bulletins publiés par US-CERT. En cas de doute sur la traduction, il est recommandé de se référer aux données fournies par les références CVE (colonne 5 du tableau).

Le CIRT-BF vous recommande fortement, si vous être un point focal pour votre organisation, de diffuser ce message à tous les membres du staff en charge de la gestion de votre Système dôInformation et des processus automatisés.

Vulnérabilités critiques

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source Info & Correctif
adobe -- adobe_reader	Lôapplication Adobe Reader Mobile avant 11.2 pour Android ne restreint pas correctement lôutilisation de JavaScript, ce qui permet à des attaquants distants dôexécuter un code arbitraire via un document PDF falsifié, un problème lié à CVE-2012-6636.	15/04/2014	9.3	CVE-2014-0514
advantech -- advantech_webaccess	De nombreuses vulnérabilités injection SQL dans DBVisitor.dll dans Advantech WebAccess avant 7.2 permettent à des attaquants distants dôexécuter des commandes SQL arbitraires via des requêtes SOAP vers des fonctions non déterminées.	12/04/2014	7.5	CVE-2014-0763
advantech -- advantech_webaccess	Un débordement de tampon dans Advantech WebAccess avant 7.2 permet à des attaquants distants dôexécuter un code arbitraire via une valeur longue du paramètre NodeName.	12/04/2014	7.5	CVE-2014-0764
advantech -- advantech_webaccess	Un débordement de pile dans Advantech WebAccess avant 7.2 permet à des attaquants distants dôexécuter un code arbitraire via une valeur longue de lôargument GotoCmd.	12/04/2014	7.5	CVE-2014-0765
advantech -- advantech_webaccess	Un débordement de pile dans Advantech WebAccess avant 7.2 permet à des attaquants distants dôexécuter un code arbitraire via une valeur longue de lôargument NodeName2.	12/04/2014	7.5	CVE-2014-0766

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source Info & Correctif
advantech -- advantech_webaccess	Un débordement de pile dans Advantech WebAccess avant 7.2 permet à des attaquants distants dôexécuter un code arbitraire via une valeur longue de lôargument AccessCode.	12/04/2014	7.5	CVE-2014-0767
advantech -- advantech_webaccess	Un débordement de pile dans Advantech WebAccess avant 7.2 permet à des attaquants distants dôexécuter un code arbitraire via une valeur longue de lôargument AccessCode2.	12/04/2014	7.5	CVE-2014-0768
advantech -- advantech_webaccess	Un débordement de pile dans Advantech WebAccess avant 7.2 permet à des attaquants distants dôexécuter un code arbitraire via une valeur longue du paramètre UserName.	12/04/2014	7.5	CVE-2014-0770
advantech -- advantech_webaccess	La méthode CreateProcess dans le contrôle ActiveX BWOCXRUN.BwocxrunCtrl.1 dans bwocxrun.ocx dans Advantech WebAccess avant 7.2 permet à des attaquants distants dôexécuter les programmes (1) setup.exe, (2) bwvbprt.exe et (3) bwvbprtl.exe à partir de noms de chemins arbitraires via un argument falsifié, comme prouvé par un nom de chemin de partage UNC.	12/04/2014	7.5	CVE-2014-0773
apache -- xalan-java	TransformerFactory dans Apache Xalan-Java avant 2.7.2 ne restreint pas correctement lôaccès à certaines propriétés lorsque FEATURE_SECURE_PROCESSING est activé, ce qui permet à des attaquants distants de contourner les restrictions attendues et de charger des classes arbitraires ou accéder à des ressources externes via une falsification de la propriété (1) xalan:content-header, (2) xalan:entities, (3) xslt:content-header, ou (4) xslt:entities ou une propriété Java qui est liée à la fonction propriété-système XSLT 1.0.	15/04/2014	7.5	CVE-2014-0107

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source Info & Correctif
blackberry -- blackberry_z10	Un débordement de pile dans une certaine fonction de décryptage dans qconnDoor sur les appareils Blackberry Z10 avec le logiciel 10.1.0.2312, lorsque le mode-developpeur a été précédemment activé, permet à des attaquants distants dôexécuter un code arbitraire via un paquet falsifié dans une session TCP sur un réseau sans fil.	12/04/2014	9.3	CVE-2014-2389
construtiva -- cis_manager_cms	Une vulnérabilité dôinjection SQL dans default.asp dans CIS Manager CMS permet à des attaquants distants dôexécuter des commandes SQL arbitraires via le paramètre TroncoID.	11/04/2014	7.5	CVE-2014-2847
emc -- cloud_tiering_appliance_software	EMC Cloud Tiering Appliance (CTA) 10 à SP1 permet à des attaquants distants de lire des fichiers arbitraires via une requête api/login contenant une déclaration dôune entité externe XML conjointement avec la référence dôune entité, en relation avec un problème XML External Entity (XXE), comme démontré par la lecture du fichier /etc/shadow.	16/04/2014	7.8	CVE-2014-0644
ioserver -- ioserver_opc_server	Le pilote slave/outstation de Modbus dans OPC Drivers 1.0.20 et précédents dans IOServer OPC Server permet à des attaquants distants de provoquer un déni de service (lecture hors limites et crash de daemon) via un paquet falsifié.	11/04/2014	7.8	CVE-2014-0777
j2k-codec -- j2k-codec	De nombreuses vulnérabilités non spécifiées dans J2k-Codec permettent à des attaquants distants dôexécuter un code arbitraire via un fichier JPEG 2000 trafiqué.	12/04/2014	10.0	CVE-2014-0349
juniper -- junos	Juniper Junos 13.2 avant 13.2R3 et 13.3 avant 13.3R1, lorsque PIM est activé, permet à des attaquants distants de provoquer un déni de service (panique du noyau et crash) via un grand nombre de paquets IGMP trafiqués.	14/04/2014	7.1	CVE-2014-0614
juniper -- junos	Enhanced Web Filtering (EWF) dans Juniper Junos avant 10.4R15, 11.4 avant 11.4R9, 12.1 avant 12.1R7, 12.1X44 avant 12.1X44-D20, 12.1X45 avant 12.1X45-D10, et	14/04/2014	7.1	CVE-2014-2714

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source Info & Correctif
	12.1X46 avant 12.1X46-D10, utilisé tel quel sur les passerelles de services des séries SRX, permet à des attaquants distants de provoquer un déni de service (crash de Flow Daemon et redémarrage) via une URL trafiquée.			
juniper -- screenos	Juniper ScreenOS 6.3 et précédentes permet à des attaquants distants de provoquer un déni de service (crash et redémarrage ou basculement) via un paquet SSL/TLS malformé.	15/04/2014	7.8	CVE-2014-2842
linux -- linux_kernel	Une condition de compétition dans le sous-système mac80211 dans le noyau Linux avant 3.13.7 permet à des attaquants distants de provoquer un déni de service (crash du système) via un trafic réseau qui interagit incorrectement avec lôétat de WLAN_STA_PS_STA (aussi appelé mode économie-dôénergie), en relation avec sta_info.c et tx.c.	14/04/2014	7.1	CVE-2014-2706
nullsoft -- winamp	Un dépassement de pile dans gen_jumpex.dll dans Winamp avant 5.64 Build 3418 permet à des attaquants distants de provoquer un déni de service (crash) et éventuellement dôexécuter un code arbitraire via un package avec un long nom du répertoire de Skin. REMARQUE : un deuxième débordement de tampon impliquant un long champ GUI Search vers ml_local.dll a aussi été rapporté. Cependant, puisquôil est seulement exploitable par lôutilisateur de lôapplication, ce problème ne devrait pas franchir les limites des privilèges à moins que Winamp soit en exécution dans un environnement hautement confiné tel que kiosk.	16/04/2014	7.5	CVE-2013-4694
oracle -- jdk	Une vulnérabilité non spécifiée dans Oracle Java SE 5.0u61, 6u71, 7u51, et 8; JRockit R27.8.1 et R28.3.1; et Java SE Embedded 7u51 permet à des attaquants distants dôaffecter la confidentialité, lôintégrité et la disponibilité via des vections inconnus liés à 2D.	15/04/2014	10.0	CVE-2014-0429

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source Info & Correctif
oracle -- jdk	Une vulnérabilité non spécifiée dans Oracle Java SE 7u51 et 8, et Java SE Embedded 7u51, permet à des attaquants distants dôaffecter la confidentialité, lôintégrité et la disponibilité via des vecteurs inconnus liés à Libraries, une vulnérabilité autre que celle de CVE-2014-0455 et CVE-2014-2402.	15/04/2014	9.3	CVE-2014-0432
oracle -- jdk	Une vulnérabilité non spécifiée dans Oracle Java SE 5.0u61, 6u71, 7u51, et 8, et Java SE Embedded 7u51, permet à des attaquants distants dôaffecter la confidentialité, lôintégrité et la disponibilité via des vecteurs liés à Libraries.	15/04/2014	7.5	CVE-2014-0446
oracle -- jdk	Une vulnérabilité non spécifiée dans Oracle Java SE 7u51 et 8 permet à des attaquants distants dôaffecter la confidentialité, lintégrité et la disponibilité via des vecteurs liés à Deployment.	15/04/2014	7.6	CVE-2014-0448
oracle -- jdk	Une vulnérabilité non spécifiée dans Oracle Java SE 5.0u61, 6u71, 7u51, and 8, and Java SE Embedded 7u51 permet à des attaquants distants dôaffecter la confidentialité, lôintégrité et la disponibilité via des vecteurs liés à AWT, une vulnérabilité différente de celle de CVE-2014-2412.	15/04/2014	7.5	CVE-2014-0451
oracle -- jdk	Une vulnérabilité non spécifiée dans Oracle Java SE 6u71, 7u51, et 8, et Java SE Embedded 7u51, permet à des attaquants distants dôaffecter la confidentialité, lôintégrité et la disponibilité via des vecteurs liés à JAX-WS, une vulnérabilité différente de celle de CVE-2014-0458 et CVE-2014-2423.	15/04/2014	7.5	CVE-2014-0452
oracle -- jdk	Une vulnérabilité non spécifiée dans Oracle Java SE 7u51 et 8, et Java SE Embedded 7u51, permet à des attaquants distants dôaffecter la confidentialité, lôintégrité et la disponibilité via des vecteurs inconnus liés à Security.	15/04/2014	7.5	CVE-2014-0454
oracle -- jdk	Une vulnérabilité non spécifiée dans Oracle Java SE 7u51 and 8, and Java SE Embedded 7u51, permet à des attaquants	15/04/2014	9.3	CVE-2014-0455

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source Info & Correctif
	distants dôaffecter la confidentialité, lôintégrité et la disponibilité via des vecteurs inconnus en relation avec Libraries, une vulnérabilité différente de celle de CVE-2014-0432 et CVE-2014-2402.			
oracle -- jdk	Une vulnérabilité non spécifiée dans Oracle Java SE 6u71, 7u51, et 8, et Java SE Embedded 7u51, permet à des attaquants distants dôaffecter la confidentialité, lôintégrité et la disponibilité via des vecteurs inconnus en relation avec Hotspot.	15/04/2014	10.0	CVE-2014-0456
oracle -- jdk	Une vulnérabilité non spécifiée dans Oracle Java SE 5.0u61, SE 6u71, 7u51, et 8; JRockit R27.8.1 et R28.3.1; et Java SE Embedded 7u51 permet à des attaquants distants dôaffecter la confidentialité, lôintégrité et la disponibilité via des vecteurs inconnus en relation avec Librairies.	15/04/2014	10.0	CVE-2014-0457
oracle -- jdk	Une vulnérabilité non spécifiée dans Oracle Java SE 6u71, 7u51, et 8, et Java SE Embedded 7u51, permet à des attaquants distants dôaffecter la confidentialité, lôintégrité et la disponibilité via des vecteurs inconnus en relation avec JAX-WS, une vulnérabilité différente de celle de CVE-2014-0452 et CVE-2014-2423.	15/04/2014	7.5	CVE-2014-0458
oracle -- jdk	Une vulnérabilité non spécifiée dans Oracle Java SE 6u71, 7u51, et 8, et Java SE Embedded 7u51, permet à des attaquants distants dôaffecter la confidentialité, lôintégrité et la disponibilité via des vecteurs inconnus en relation avec Librairies.	15/04/2014	9.3	CVE-2014-0461
oracle -- jdk	Une vulnérabilité non spécifiée dans Oracle Java SE 7u51 et 8, et Java SE Embedded 7u51, permet à des attaquants distants dôaffecter la confidentialité, lôintégrité et la disponibilité via des vecteurs inconnus en relation avec Hotspot.	15/04/2014	9.3	CVE-2014-2397

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source Info & Correctif
oracle -- jdk	Une vulnérabilité non spécifiée dans Oracle Java SE 7u51 et 8, et Java SE Embedded 7u51 permet à des attaquants distants dôaffecter la confidentialité, lôintégrité et la disponibilité via des vecteurs inconnus en relation avec Librairies, une vulnérabilité différente de celle de CVE-2014-0432 et CVE-2014-0455.	15/04/2014	7.5	CVE-2014-2402
oracle -- database_server	Une vulnérabilité non spécifiée dans la composante Core RDBMS dans Oracle Database Server 11.1.0.7, 11.2.0.3, 11.2.0.4, et 12.1.0.1 permet à des utilisateurs authentifiés à distance dôaffecter la confidentialité, lôintégrité et la disponibilité via des vecteurs inconnus en relation avec les privilèges « Advisor » et « Select Any Dictionary ».	15/04/2014	8.5	CVE-2014-2406
oracle -- jdk	Une vulnérabilité non spécifiée dans Oracle Java SE 8 permet à des attaquants distants dôaffecter la confidentialité, lôintégrité et la disponibilité via des vecteurs inconnus en relation avec JavaFX.	15/04/2014	9.3	CVE-2014-2410
oracle -- jdk	Une vulnérabilité non spécifiée dans Oracle Java SE 5.0u61, 6u71, SE 7u51, et 8, et Java SE Embedded 7u51 permet à des attaquants distants dôaffecter la confidentialité, lôintégrité et la disponibilité via des vecteurs inconnus en relation avec AWT, une vulnérabilité différente de celle de CVE-2014-0451.	15/04/2014	7.5	CVE-2014-2412
oracle -- jdk	Une vulnérabilité non spécifiée dans Oracle Java SE 6u71, 7u51, et 8, et Java SE Embedded 7u51 permet à des attaquants distants dôaffecter la confidentialité, lôintégrité et la disponibilité via des vecteurs en relation avec JAXB.	15/04/2014	7.5	CVE-2014-2414
oracle -- javafx	Une vulnérabilité non spécifiée sans Oracle Java SE 5.0u61, 6u71, 7u51, et 8; JavaFX 2.2.51; et Java SE Embedded 7u51 permet à des attaquants distants dôaffecter la confidentialité, lôintégrité et la disponibilité via des vecteurs inconnus en relation avec 2D.	15/04/2014	10.0	CVE-2014-2421

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source Info & Correctif
oracle -- jdk	Une vulnérabilité non spécifiée dans Oracle Java SE 6u71, 7u51, et 8, et Java SE Embedded 7u51 permet à des attaquants distants dôaffecter la confidentialité, lôintégrité et la disponibilité via des vecteurs en relation avec JAX-WS, une vulnérabilité différente de celle de CVE-2014-0452 et CVE-2014-0458.	15/04/2014	7.5	CVE-2014-2423
oracle -- jdk	Une vulnérabilité non spécifiée dans Oracle Java SE 5.0u61, 6u71, 7u51, et 8, et Java SE Embedded 7u51 permet à des attaquants distants dôaffecter la confidentialité, lôintégrité et la disponibilité via des vecteurs inconnus en relation avec Sound.	15/04/2014	7.5	CVE-2014-2427
oracle -- jdk	Une vulnérabilité non spécifiée dans Oracle Java SE 6u71, 7u51, et 8, et Java SE Embedded 7u51 permet à des attaquants distants dôaffecter la confidentialité, lôintégrité et la disponibilité via des vecteurs inconnus en relation avec Deployment.	15/04/2014	7.6	CVE-2014-2428
oracle -- fusion_middleware	Une vulnérabilité non spécifiée dans la composante Oracle WebLogic Server dans Oracle Fusion Middleware 10.0.2.0, 10.3.6.0, 12.1.1.0 et 12.1.2.0 permet à des attaquants distants dôaffecter la confidentialité, lôintégrité et la disponibilité via des vecteurs en relation avec WLS Security.	15/04/2014	7.5	CVE-2014-2470
orbitscripts -- orbit_open_ad_server	Une vulnérabilité injection SQL dans OrbitScripts Orbit Open Ad Server avant 1.1.1 permet à des attaquants distants dôexécuter des commandes SQL arbitraires via le paramètre site_directory_sort_field vers guest/site_directory.	11/04/2014	7.5	CVE-2014-2540
osisoft -- pi_interface	DNP Master Driver dans OSIsoft PI Interface avant 3.1.2.54 pour DNP3 permet à des attaquants distants de provoquer un déni de service (fermeture de lôinterface) via un paquet TCP trafiqué.	12/04/2014	7.1	CVE-2013-2809

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source Info & Correctif
paperthin -- commonspot_content_server	PaperThin CommonSpot avant 7.0.2 et 8.x avant 8.0.3 permet à des attaquants distants de contourner les restrictions dôaccès prévues via une requête directe.	15/04/2014	7.5	CVE-2014-2859
paperthin -- commonspot_content_server	De nombreuses traversées de chemins absolues dans PaperThin CommonSpot avant 7.0.2 et 8.x et 8.0.3 permettent à des attaquants distants dôavoir un impact non spécifié via un nom de répertoire complet dans un paramètre.	15/04/2014	10.0	CVE-2014-2863
paperthin -- commonspot_content_server	De nombreuses vulnérabilités traversées de répertoires dans PaperThin CommonSpot avant 7.0.2 et 8.x avant 8.0.3 permettent à des attaquants distants dôavoir un impact non spécifié via un paramètre filename contenant des séquences de traversées de répertoires.	15/04/2014	10.0	CVE-2014-2864
paperthin -- commonspot_content_server	PaperThin CommonSpot avant 7.0.2 et 8.x avant 8.0.3 permet à des attaquants distants de contourner les restrictions dôaccès prévues via le caractère ' ' comme prouvé par lôutilisation de ce caractère dans un nom de chemin sur le lecteur contenant le répertoire racine du web de lôinstallation ColdFusion.	15/04/2014	7.5	CVE-2014-2865
paperthin -- commonspot_content_server	PaperThin CommonSpot avant 7.0.2 et 8.x avant 8.0.3 se fonde sur un code client JavaScript pour les restrictions dôaccès, ce qui permet à des attaquants distants de réaliser des opérations non spécifiées en modifiant ce code.	15/04/2014	10.0	CVE-2014-2866
paperthin -- commonspot_content_server	Une vulnérabilité de non restriction de transfert de fichier dans PaperThin CommonSpot avant 7.0.2 et 8.x avant 8.0.3 permet à des attaquants distants dôexécuter un code arbitraire en transférant une page ColdFusion, et y accéder ainsi via des vecteurs non spécifiés.	15/04/2014	10.0	CVE-2014-2867
paperthin -- commonspot_content_server	PaperThin CommonSpot avant 7.0.2 et 8.x avant 8.0.3 permet à des attaquants distants de modifier le flux dôexécution du code de ColdFusion en utilisant une requête	15/04/2014	7.5	CVE-2014-2868

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source Info & Correctif
	HTTP GET pour y placer une variable de ColdFusion.			
paperthin -- commonspot_content_server	PaperThin CommonSpot avant 7.0.2 et 8.x avant 8.0.3 permet à des attaquants distants dœexécuter un code arbitraire via les métacaractères du shell dans un contexte non spécifié.	15/04/2014	10.0	CVE-2014-2874
pivotx -- pivotx	De nombreuses vulnérabilités de non restriction de transfert de fichier dans fileupload.php dans PivotX avant 2.3.9 permettent à des utilisateurs authentifiés à distance dœexécuter un code PHP arbitraire en transférant un fichier via une extension (1) .php ou (2) .php# et y accéder ainsi via des vecteurs non spécifiés.	15/04/2014	7.5	CVE-2014-0342
sophos -- web_appliance_firmware	La boîte de dialogue Change Password (change_password) dans Sophos Web Appliance avant 3.8.2 permet à des utilisateurs authentifiés à distance de changer le mot de passe de lœutilisateur admin via des requêtes trafiquées.	11/04/2014	8.5	CVE-2014-2849
sophos -- web_appliance_firmware	La page de configuration de lœinterface réseau (netinterface) dans Sophos Web Appliance avant 3.8.2 permet à des administrateurs distants dœexécuter des commandes arbitraires via les métacaractères du shell dans le paramètre address.	11/04/2014	8.5	CVE-2014-2850
suse -- kiwi	kiwi avant 4.98.08, tel quœutilisé dans SUSE Studio Onsite 1.2 avant 1.2.1 et SUSE Studio Extension pour System z 1.2 avant 1.2.1, permet à des attaquants dœexécuter des commandes arbitraires via les métacaractères du shell dans le chemin dœun fichier de superposition, en relation avec chown.	16/04/2014	7.5	CVE-2011-3180
suse -- kiwi	kiwi avant 4.85.1, tel quœutilisé dans SUSE Studio Onsite 1.2 avant 1.2.1 et SUSE Studio Extension pour System z 1.2 avant 1.2.1, permet à des attaquants dœexécuter des commandes arbitraires comme prouvé par "double quotes dans kiwi_oemtitle de .profile."	16/04/2014	7.5	CVE-2011-4192

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source Info & Correctif
suse -- kiwi	kiwi avant 4.98.05, tel quôutilisé dans SUSE Studio Onsite 1.2 avant 1.2.1 et SUSE Studio Extension pour System z 1.2 avant 1.2.1, permet à des attaquants dôexécuter des commandes arbitraires via les métacaractères du shell dans un nom dôimage.	16/04/2014	7.5	CVE-2011-4195
vmware -- vsphere_client	VMware vSphere Client 4.0, 4.1, 5.0 avant Update 3, et 5.1 avant Update 2 ne valide pas correctement les mise-à-jour vers les fichiers des clients, ce qui permet à des attaquants distants de déclencher le téléchargement et lôexécution dôun programme arbitraire via des vecteurs non spécifiés.	11/04/2014	9.3	CVE-2014-1209
wellintech -- kingscada	Un dépassement de pile dans WellinTech KingSCADA avant 3.1.2.13 permet à des attaquants distants dôexécuter un code arbitraire via un paquet trafiqué.	12/04/2014	10.0	CVE-2014-0787
xangati -- xangati_software_release	De nombreuses vulnérabilités traversées de répertoire dans Xangati XSR avant 11 et XNR avant 7 permettent à des attaquants distants de lire des fichiers arbitraires via des .. (point point) dans (1) le paramètre file dans une action getUpgradeStatus vers servlet/MGConfigData, (2) le paramètre download dans une action download vers servlet/MGConfigData (3) le paramètre download dans une action port_svc vers servlet/MGConfigData, (4) le paramètre file dans une action getfile vers servlet/Installer, ou (5) le paramètre binfile vers servlet/MGConfigData.	15/04/2014	7.8	CVE-2014-0358
xangati -- xangati_software_release	Xangati XSR avant 11 et XNR avant 7 permet à des attaquants distants dôexécuter des commandes arbitraires via les métacaractères du shell dans le paramètre params de gui_input_test.pl vers servlet/Installer.	15/04/2014	9.0	CVE-2014-0359
zyxel -- n300_netusb_nbg-419n	Le routeur ZyXEL Wireless N300 NetUSB NBG-419N avec le micrologiciel 1.00(BFQ.6)C0 a un mot de passe qweasdzxc codé en dur pour un compte non spécifié, ce qui permet à des attaquants distants dôobtenir un accès au login	15/04/2014	7.8	CVE-2014-0354

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source Info & Correctif
	dôindex.asp via une requête HTTP.			
zyxel -- n300_netusb_nbg-419n	De nombreux débordments de pile dans le routeur ZyXEL Wireless N300 NetUSB NBG-419N doté du micrologiciel 1.00(BFQ.6)C0 permettent à des attaquants man-in-the-middle dôexécuter un code arbitraire via (1) un long attribut temp dans lôélément yweather:condition dans un fichier forecastrss qui est traité par la fonction checkWeather ; la variable (2) WeatherCity ou (3) WeatherDegree vers la fonction detectWeather ; une entrée non spécifiée vers la fonction (4) UpnpAddRunRLQoS, (5) UpnpDeleteRunRLQoS, ou (6) UpnpDeletePortCheckType ; ou (7) la commande SET COUNTRY udps.	15/04/2014	7.9	CVE-2014-0355
zyxel -- n300_netusb_nbg-419n	Le routeur ZyXEL Wireless N300 NetUSB NBG-419N doté du micrologiciel 1.00(BFQ.6)C0 permet à des attaquants distants dôexécuter un code arbitraire via les métacaractères du shell dans lôentrée de la fonction (1) detectWeather, (2) set_language, (3) SystemCommand, ou (4) NTPSyncWithHost dans management.c, ou la commande (5) SET COUNTRY, (6) SET WLAN SSID, (7) SET WLAN CHANNEL, (8) SET WLAN STATUS, ou (9) SET WLAN COUNTRY udps.	15/04/2014	7.9	CVE-2014-0356

Retour haut de page

Vulnérabilités majeures

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source Info & Correctif
advanced_package_tool -- advanced_package_tool	La méthode pkgAcqMetaClearSig::Failed dans apt-pkg/acquire-item.cc dans Advanced Package Tool (APT) 0.8.11 à 0.8.15.10 et 0.8.16 avant 0.8.16~exp13, lorsquôelle est mise à jour à partir des	15/04/2014	4.3	CVE-2012-0214

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source Info & Correctif
	dépôts qui utilisent des fichiers InRelease, permet à des attaquants man-in-the-middle dôinstaller des packages arbitraires en empêchant un utilisateur de télécharger un nouveau fichier InRelease, ce qui laisse le fichier InRelease original actif and rend plus compliqué de détecter que le fichier Packages est modifié et non signé.			
advantech -- advantech_webaccess	La méthode OpenUrlToBuffer dans le contrôle ActiveX BWOCXRUN.BwocxrunCtrl.1 dans bwocxrun.ocx dans Advantech WebAccess before 7.2 permet à des attaquants distants de lire des fichiers arbitraires via une URL « fichier: ».	12/04/2014	5.0	CVE-2014-0771
advantech -- advantech_webaccess	La méthode OpenUrlToBufferTimeout dans le contrôle ActiveX BWOCXRUN.BwocxrunCtrl.1 dans bwocxrun.ocx dans Advantech WebAccess before 7.2 permet à des attaquants distants de lire des fichiers arbitraires via une URL « fichier: ».	12/04/2014	5.0	CVE-2014-0772
amos_benari -- rbovirt	Le gem rbovirt avant 0.0.24 pour Ruby utilise le gem rest-client avec une vérification SSL desactivée, ce qui permet à des attaquants distants de mener des attaques man-in-the-middle via des vecteurs non spécifiés.	17/04/2014	6.8	CVE-2014-0036
amtelco -- misecuremessages	Amtelco miSecureMessages permet à des attaquants distants de lire les messages dôutilisateurs arbitraires via une requête XML contenant une clé de licence valide et une valeur de contactID modifiée, comme démontrée par une requête venant dôune application iOS ou Android.	15/04/2014	5.0	CVE-2014-0357
apache -- http_server	Le module mod_headers dans Apache HTTP Server 2.2.22 permet à des attaquants distants de contourner les directives "RequestHeader unset" en plaçant un entête dans la portion du trailer des données envoyées avec « chunked transfer coding ». REMARQUE : Le vendeur affirme que « ceci nôest pas un problème de sécurité dans httpd en tant que tel »	15/04/2014	5.0	CVE-2013-5704
apache -- syncope	Apache Syncope 1.0.0 avant 1.0.9 et 1.1.0 avant 1.1.7 permet à des administrateurs dôexécuter un code Java arbitraire via des	17/04/2014	6.5	CVE-2014-0111

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source Info & Correctif
	vecteurs liés aux expressions "derived schema definition," "user / role templates," et "account links of resource mappings." dôApache Commons JEXL			
apps4u@android -- sd_card_manager	Une vulnérabilité traversée de répertoire dans lôapplication apps4u@android SD Card Manager avant 20140224 pour Android permet à des attaquants dôécraser ou créer des fichiers arbitraires via un nom de fichier falsifié.	11/04/2014	5.8	CVE-2014-1969
bzip -- bzip2	La commande bzexe dans bzip2 1.0.5 et antérieures génère des exécutables compressés qui ne manipulent pas correctement les fichiers temporaires durant lôextraction, ce qui permet à des utilisateurs locaux dôexécuter un code arbitraire en créant dôavance un répertoire temporaire.	16/04/2014	4.6	CVE-2011-4089
cambridge_enterprise -- jbig-kit	Un débordement de pile dans la fonction jbg_dec_in dans libjbig/jbig.c dans JBIG-KIT avant 2.1 permet à des attaquants distants de provoquer un déni de service (crash dôapplication) et éventuellement exécuter un code arbitraire via un fichier image trafiqué.	11/04/2014	6.8	CVE-2013-6369
canonical -- libpam-modules	Une vulnérabilité de chemin de recherche non sure (aussi connu sous lôappelation module MOTD) dans libpam-modules avant 1.1.3-2ubuntu2.1 sur Ubuntu 11.10, avant 1.1.2-2ubuntu8.4 sur Ubuntu 11.04, avant 1.1.1-4ubuntu2.4 sur Ubuntu 10.10, avant 1.1.1-2ubuntu5.4 sur Ubuntu 10.04 LTS, et avant 0.99.7.1-5ubuntu6.5 sur Ubuntu 8.04 LTS, lorsque certaines configurations sont utilisées telle que "session optional pam_motd.so", permet à des utilisateurs locaux dôobtenir des privilèges en modifiant la variable dôenvironnement PATH pour référencer une commande malicieuse, comme prouvé via uname.	15/04/2014	6.9	CVE-2011-3628
cisco -- ons_15454	Les cartes-contrôleurs de Cisco ONS 15454 dotées du logiciel 9.6 et antérieurs permettent à des attaquants distants de provoquer un déni de service (interruption du service dôécriture sur le flash) via une attaque TCP FIN qui déclenche un	12/04/2014	5.0	CVE-2014-2139

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source Info & Correctif
	épuisement des descripteurs de fichier, aussi connu sous lâappelation Bug ID CSCug97315.			
cisco -- ons_15454	Les cartes-contrôleurs de Cisco ONS 15454 dotées du logiciel 9.6 et antérieurs permettent à des attaquants distants de provoquer un déni de service (réinitialisation de la carte) via une attaque TCP FIN qui déclenche un épuisement des descripteurs de fichier et un échec dâouverture dâun pipe CAL, aussi connu sous lâappelation de Bug ID CSCug97348.	12/04/2014	5.0	CVE-2014-2140
cisco -- ons_15454	Les cartes-contrôleurs de Cisco ONS 15454 dotées du logiciel 10.0 et antérieurs permettent à des attaquants distants de provoquer un déni de service (redémarrage à chaud de la carte) via un URI HTTP trafiqué, aussi connu sous lâappelation de Bug ID CSCun06870.	12/04/2014	5.0	CVE-2014-2142
dell -- sonicwall_email_security	De nombreuses vulnérabilités cross-site scripting (XSS) dans Dell SonicWALL Email Security 7.4.5 et antérieures permettent à des administrateurs authentifiés à distance dâinjecter un script web ou HTML arbitraire via (1) le paramètre uploadPatch vers la page System/Advanced (settings_advanced.html) ou (2) le paramètre uploadLicenses dans la page License management (settings_upload_dlicense.html).	17/04/2014	4.3	CVE-2014-2879
elfutils_project -- elfutils	Un débordement dâentier dans la fonction check_section dans dwarf_begin_elf.c dans la bibliothèque libdw, tel quâutilisé dans elfutils 0.153 et peut-être jusquâà 0.158, permet à des attaquants distants de provoquer un déni de service (crash dâapplication) ou éventuellement dâexécuter un code arbitraire via une section debug compressée malformée dans un fichier ELF, ce qui déclenche un débordement de tas dans le tampon.	11/04/2014	6.8	CVE-2014-0172
emc -- rsa_bsafe	EMC RSA BSAFE Micro Edition Suite (MES) 3.2.x avant 3.2.6 et 4.0.x avant 4.0.5 ne valide pas correctement les chaines du certificat X.509, ce qui permet à des attaquants man-in-the-middle dâusurper des serveurs SSL via une chaine de certificat	11/04/2014	5.8	CVE-2014-0636

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source Info & Correctif
	falsifiée.			
emc -- documentum_content_server	EMC Documentum Content Server avant 6.7 SP1 P26, 6.7 SP2 avant P13, 7.0 avant P13, et 7.1 avant P02 permet à des utilisateurs authentifiés à distance de contourner les restrictions dôaccès prévues et lire des méta-données à partir de certains dossiers via des vecteurs non spécifiés.	15/04/2014	5.5	CVE-2014-0642
emc -- cloud_tiering_appliance_software	EMC Cloud Tiering Appliance (CTA) 9.x à 10 SP1 et File Management Appliance (FMA) 7.x stockent des hashs DES pour les mots de passe des comptes root, super et admin, ce qui permet plus facilement à des attaquants selon le contexte dôobtenir des informations sensibles via une attaque brute force.	16/04/2014	4.7	CVE-2014-0645
eucalyptus -- eucalyptus	Les APIs des services web dans Eucalyptus 2.0 à 3.4.1 permettent à des attaquants distants de provoquer un déni de service via des vecteurs liés au « code de nettoyage de la connexion réseau » et (1) Cloud Controller (CLC), (2) Walrus, (3) Storage Controller (SC), et (4) VMware Broker (VB).	15/04/2014	5.0	CVE-2013-4768
freebsd -- freebsd	Le serveur NFS (de nfsserver) sous FreeBSD 8.3 à 10.0 n'acquiert pas de verrous dans le bon ordre lors de la conversion d'un descripteur de fichier de répertoire pour un vnode, qui permet aux utilisateurs à distance authentifiés afin de causer un déni de service (impasse) par des vecteurs impliquant un fil qui utilise l'ordre de verrouillage correct.	16/04/2014	4.0	CVE-2014-1453
gopivotal -- grails	La configuration par défaut du plugin Resources 1.0.0 avant 1.2.6 pour Pivotal Grails 2.0.0 avant 2.3.6 ne restreint pas correctement lôaccès aux fichiers dans le répertoire WEB-INF, ce qui permet à des attaquants distants dôobtenir des informations sensibles via une requête directe. REMARQUE : ce numéro dôidentification a été scindé dû à des chercheurs différents et à des types de vulnérabilités différentes. Voir CVE-2014-2857 pour la variante META-INF et CVE-2014-2858 pour la traversée de répertoire.	15/04/2014	5.0	CVE-2014-0053

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source Info & Correctif
gopivotal -- grails	La configuration par défaut du plugin Resources 1.0.0 avant 1.2.6 pour Pivotal Grails 2.0.0 avant 2.3.6 ne restreint pas correctement lôaccès aux fichiers dans le répertoire META-INF, ce qui permet à des attaquants distants dôobtenir des informations sensibles via une requête directe. REMARQUE : ce numéro dôidentification a été scindé à partir de CVE-2014-0053 dû à des chercheurs différents par ADT5.	15/04/2014	5.0	CVE-2014-2857
gopivotal -- grails	Une vulnérabilité traversée de répertoire dans le plugin Resources 1.0.0 avnt 1.2.6 pour Pivotal Grails 2.0.0 à 2.3.6 permet à des attaquants distants dôobtenir des informations sensibles via des vecteurs non spécifiés liés à "configured block." REMARQUE : ce problème a été scindé de la référence CVE-2014-0053 par ADT2 en raison des différences de types de vulnérabilité.	15/04/2014	5.0	CVE-2014-2858
haxx -- curl	La configuration par défaut dans cURL et libcurl 7.10.6 avant 7.36.0 réutilise des connexions (1) SCP, (2) SFTP, (3) POP3, (4) POP3S, (5) IMAP, (6) IMAPS, (7) SMTP, (8) SMTPS, (9) LDAP, et (10) LDAPS, ce qui pourrait permettre à des attaquants selon le contexte de se connecter comme dôautres utilisateurs via une requête, un problème similaire à celui de CVE-2014-0015.	15/04/2014	6.4	CVE-2014-0138
haxx -- curl	cURL and libcurl 7.1 avant 7.36.0, lorsque les bibliothèques pour OpenSSL, axtls, qsossl or gskit sont utilisées pour TLS, reconnaissent une adresse IP générique dans le sujet du champ Common Name (CN) dôun certificat X.509, ce qui pourrait permettre à des attaquants man-in-the-middle dôusurper des serveurs SSL arbitraires via un certificat falsifié délivré par une Autorité de Certification légitime.	15/04/2014	5.8	CVE-2014-0139
ibm -- messagesight_jms_client	Le serveur dans IBM MessageSight 1.x avant 1.1.0.0-IBM-IMA-IT01015 permet à des attaquants distants de provoquer un déni de service (crash de demon et perte de données de message) via des entêtes malformés lors de la mise-à-jour dôune connexion	15/04/2014	4.3	CVE-2014-0921

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source Info & Correctif
	WebSockets.			
ibm -- messagesight_jms_client	IBM MessageSight 1.x avant 1.1.0.0-IBM-IMA-IT01015 permet à des attaquants distants de provoquer un déni de service (consommation ressource) via des données de WebSockets MQ Telemetry Transport (MQTT).	15/04/2014	4.3	CVE-2014-0922
ibm -- messagesight_jms_client	IBM MessageSight 1.x avant 1.1.0.0-IBM-IMA-IT01015 permet à des attaquants distants de provoquer un déni de service (redémarraque de demon) via des données dôauthentification de MQ Telemetry Transport (MQTT).	15/04/2014	4.3	CVE-2014-0923
ibm -- messagesight_jms_client	IBM MessageSight 1.x avant 1.1.0.0-IBM-IMA-IT01015 ne vérifie pas que tous les caractères du mot de passe sont corrects, ce qui permet plus facilement à des utilisateurs authentifiés à distance de contourner les restrictions dôaccès prévues en se basant sur la connaissance des sous-caractères du mot de passe.	15/04/2014	4.6	CVE-2014-0924
juniper -- srx100	Une vulnérabilité non spécifiée dans Juniper Junos avant 11.4R10-S1, avant 11.4R11, 12.1X44 avant 12.1X44-D26, 12.1X44 avant 12.1X44-D30, 12.1X45 avant 12.1X45-D20, et 12.1X46 avant 12.1X46-D10, lorsque Dynamic IPsec VPN est configuré, permet à des attaquants distants de provoquer un déni de service (échecs des nouvelles connexions Dynamic VPN et consommation CPU et disque) via des vecteurs inconnus.	14/04/2014	5.0	CVE-2014-0612
juniper -- junos	Une vulnérabilité Cross-site scripting (XSS) dans J-Web in Juniper Junos avant 11.4R11, 11.4X27 avant 11.4X27.62 (BBE), 12.1 avant 12.1R9, 12.1X44 avant 12.1X44-D35, 12.1X45 avant 12.1X45-D25, 12.1X46 avant 12.1X46-D20, 12.2 avant 12.2R7, 12.3 avant 12.3R6, 13.1 avant 13.1R4, 13.2 avant 13.2R3, et 13.3 avant 13.3R1 permet à des attaquants distants dôinjecter un script web ou HTML arbitraire via des vecteurs non spécifiés.	14/04/2014	4.3	CVE-2014-2711
juniper -- junos	Une vulnérabilité Cross-site scripting (XSS) dans J-Web in Juniper Junos avant 10.0S25, 10.4 avant 10.4R10, 11.4 avant 11.4R11, 12.1 avant 12.1R9, 12.1X44 avant 12.1X44-D30,	14/04/2014	4.3	CVE-2014-2712

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source Info & Correctif
	12.1X45 avant 12.1X45-D20, 12.1X46 avant 12.1X46-D10, et 12.2 avant 12.2R1 permet à des attaquants distants dôinjecter un script web ou HTML arbitraire via des paramètres non spécifiés vers index.php.			
juniper -- junos	Juniper Junos avant 11.4R11, 12.1 avant 12.1R9, 12.2 avant 12.2R7, 12.3R4 avant 12.3R4-S3, 13.1 avant 13.1R4, 13.2 avant 13.2R2, et 13.3 avant 13.3R1, tel quôutilisé dans les Séries MX et les routeurs T4000, permet à des attaquants distants de provoquer un déni de service (redémarrage PFE) via un paquet IP trafiqué vers certains modules (1) Trio ou (2) Cassis-based Packet Forwarding Engine (PFE).	14/04/2014	5.0	CVE-2014-2713
katello -- katello	Le contrôleur des utilisateurs dans Katello 1.5.0-14 et antérieurs, dans Red Hat Satellite, ne vérifie pas lôautorisation pour lôaction update_roles, ce qui permet à des utilisateurs authentifiés à distance dôobtenir des privilèges en configurant un compte utilisateur à un compte administrateur.	17/04/2014	6.5	CVE-2013-2143
kbd-project -- kbd	Le script init dans kbd, peut-être 1.14.1 et antérieur, permet à des utilisateurs locaux dôécraser des fichiers arbitraires via une attaque symlink dans /dev/shm/defkeymap.map.	16/04/2014	6.3	CVE-2011-0460
kokuyo -- camiapp	Content Provider dans lôapplication KOKUYO CamiApp 1.21.1 et antérieur pour Android permet à des attaquants de contourner les restrictions dôaccès prévues et lire les informations de la base de données via une application trafiquée.	15/04/2014	5.8	CVE-2014-1986
linux -- linux_kernel	drivers/vhost/net.c dans le noyau Linux avant 3.13.10, lorque ques des tampons fusionnables sont désactivés, ne valide pas correctement les longueurs des paquets, ce qui permet à des utilisateurs dôOS hôtes de provoquer un déni de service (corruption mémoire et crash de lôOS hôte) ou éventuellement obtenir des privilèges sur lôOS de lôhôte via des paquets trafiqués, en relation avec les fonctions handle_rx et get_rx_bufs.	14/04/2014	5.5	CVE-2014-0077

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source Info & Correctif
linux -- linux_kernel	La fonction ioapic_deliver dans virt/kvm/ioapic.c dans le noyau Linux jusquôà 3.14.1 ne valide pas correctement la valeur return de kvm_irq_delivery_to_apic, ce qui permet à des utilisateurs des OS hôtes de provoquer un déni de service (crash de lôOS hôte) via une entrée trafiquée dans la table de redirection dôun APIC I/O. REMARQUE : le code affecté était déplacé vers la fonction ioapic_service avant que la vulnérabilité ne soit annoncée.	14/04/2014	5.5	CVE-2014-0155
linux -- linux_kernel	La fonction cma_req_handler dans drivers/infiniband/core/cma.c dans le noyau Linux 3.14.x à 3.14.1 tente de résoudre une adresse RDMA sur Converged Ethernet (aussi connu sous lôappelation RoCE) qui est correctement résolue dans un module différent, ce qui permet à des attaquants distants de provoquer un déni de service (déréférencement incorrecte de pointeur et crash système) via un trafic réseau fabriqué.	14/04/2014	4.6	CVE-2014-2739
linux -- linux_kernel	Un débordement dôentier dans la fonction ping_init_sock dans net/ipv4/ping.c dans le noyau Linux jusquôà 3.14.1 permet à des utilisateurs locaux de provoquer un déni de service (use-after-free et crash système) ou éventuellement obtenir des privilèges via une application trafiquée qui sôappuie sur un compteur de référence mal géré.	14/04/2014	6.9	CVE-2014-2851
linuxfoundation -- cups-filters	cups-browsed dans cups-filters 1.0.41 avant 1.0.51 permet à des imprimantes IPP distantes dôexécuter des commandes arbitraires via les métacaractères du shell dans le (1) model ou (2) PDL, en relation avec "System V interface scripts generated for queues."	17/04/2014	5.8	CVE-2014-2707
modsecurity -- modsecurity	apache2/modsecurity.c dans ModSecurity before 2.7.6 permet à des attaquants distants de contourner les règles en utilisant « chunked transfer coding » avec une valeur Chunked capitalisée dans lôentête HTTP Transfer-Encoding	15/04/2014	5.0	CVE-2013-5705
mysql -- mysql	Une vulnérabilité non spécifiée dans la composante MySQL Server dans Oracle MySQL 5.5.35 et antérieurs et 5.6.15 et antérieurs permet à des utilisateurs authentifiés à distance	15/04/2014	4.0	CVE-2014-0384

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source Info & Correctif
	dôaffecter la disponibilité via des vecteurs liés à XML.			
mysql -- mysql	Une vulnérabilité non spécifiée dans Oracle MySQL Server 5.5.35 et antérieurs et 5.6.15 et antérieurs permet à des utilisateurs authentifiés à distance dôaffecter la disponibilité via des vecteurs inconnus en relation avec Partition.	15/04/2014	4.0	CVE-2014-2419
mysql -- mysql	Une vulnérabilité non spécifiée dans Oracle MySQL Server 5.5.36 et antérieurs et 5.6.16 et antérieurs permet à des utilisateurs authentifiés à distance dôaffecter la confidentialité, lôintégrité et la disponibilité via des vecteurs liés à RBR.	15/04/2014	6.0	CVE-2014-2436
mysql -- mysql	Une vulnérabilité non spécifiée dans la composante MySQL Client dans Oracle MySQL 5.5.36 et antérieurs et 5.6.16 et antérieurs permet à des attaquants distants dôaffecter la confidentialité, lôintégrité et la disponibilité via des vecteurs inconnus.	15/04/2014	5.1	CVE-2014-2440
net-snmp -- net-snmp	Le sous-agent AgentX dans Net-SNMP avant 5.4.4 permet à des attaquants distants de provoquer un déni de service (plantage) par envoi de requêtes multi-objets avec un Object ID (OID) contenant plus de sous-IDs que les requêtes précédentes, une vulnérabilité différente de celle de la référence CVE-2012-6151.	17/04/2014	5.0	CVE-2014-2310
openafs -- openafs	Un débordement de tampon dans la procédure dôappel à distance (RPC) GetStatistics64 dans OpenAFS 1.4.8 avant 1.6.7 permet à des attaquants distants de provoquer un déni de service (crash) via un argument falsifié de statsVersion.	14/04/2014	5.0	CVE-2014-0159
openafs -- openafs	OpenAFS avant 1.6.7 retarde le fil dôécoute quand un RXS_CheckResponse échoue, ce qui permet à des attaquants distants de provoque un déni de service (dégradation de performance) via un paquet invalide.	14/04/2014	5.0	CVE-2014-2852
openfabrics -- ibutils	Une vulnérabilité chemin de recherche non fiable dans un certain script de Red Hat build pour lôexécutable ibmssh dans les packages ibutils avant ibutils-1.5.7-2.el6 dans Red Hat Enterprise	15/04/2014	4.4	CVE-2008-3277

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source Info & Correctif
	Linux (RHEL) 6 et ibutils-1.2-11.2.el5 dans Red Hat Enterprise Linux (RHEL) 5 permet à des utilisateurs locaux dôobtenir des privilèges via un programme Cheval de Troyes dans refix/lib/, en relation avec une configuration incorrecte de RPATH dans lôentête ELF.			
openssl -- openssl	Une condition de compétition dans la fonction ssl3_read_bytes dans s3_pkt.c dans OpenSSL jusquôà 1.0.1g, lorsque SSL_MODE_RELEASE_BUFFERS est activé, permet à des attaquants distants dôinjecter des données entre les sessions ou provoquer un déni de service (use-after-free et erreur dôanalyse) via une connexion SSL dans un environnement multithread.	14/04/2014	4.0	CVE-2010-5298
openstack -- python-keystoneclient	Le middleware auth_token dans la bibliothèque client OpenStack Python pour Keystone (aussi connue sous lôappelation python-keystoneclient) avant 0.7.0 ne récupère pas correctement les jetons utilisateur de memcache, ce qui permet à des utilisateurs authentifiés à distance dôobtenir des priviligèes dans des circonstances opportunistes via un grand nombre de requêtes, en relation avec une « interaction entre eventlet et python-memcached ».	15/04/2014	6.0	CVE-2014-0105
openstack -- horizon	Une vulnérabilité Cross-site scripting (XSS) dans le dashboard dôHorizon Orchestration dans OpenStack Dashboard (aussi connu sous lôappelation de Horizon) 2013.2 avant 2013.2.4 et icehouse avant icehouse-rc2 permet à des attaquants distants dôinjecter un script web ou HTML via le champ de description du modèle Heat.	15/04/2014	4.3	CVE-2014-0157
openstack -- compute	Lôimplémentation du groupe de sécurité de lôAPI Nova EC2 dans OpenStack Compute (Nova) 2013.1 avant 2013.2.4 et icehouse avant icehouse-rc2 nôapplique pas les politiques RBAC pour (1) add_rules, (2) remove_rules, (3) destroy et dôautres méthodes non spécifiées dans compute/api.py lorsque les politiques par défaut sont utilisées, ce qui permet à des utilisateurs authentifiés	15/04/2014	6.0	CVE-2014-0167

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source Info & Correctif
	à distance dôobtenir des privilèges via ces requêtes de lôAPI.			
openstack -- keystone	LôAPI V3 dans OpenStack Identity (Keystone) 2013.1 avant 2013.2.4 et icehouse avant icehouse-rc2 permet à des attaquants distants de provoquer un déni de service (consommation CPU) via un grand nombre de la même méthode dôauthentification dans une requête, aussi connu sous "authentication chaining."	15/04/2014	5.0	CVE-2014-2828
oracle -- fusion_middleware	Une vulnérabilité non spécifiée dans les Containers dôOracle pour la composante J2EE dans Oracle Fusion Middleware 10.1.3.5 permet à des attaquants distants dôaffecter lôintégrité via des vecteurs liés à la manipulation des requêtes HTTP, une vulnérabilité différente de celle de CVE-2014-0426.	15/04/2014	4.3	CVE-2014-0413
oracle -- fusion_middleware	Une vulnérabilité non spécifiée dans les Containers dôOracle pour la composante J2EE dans Oracle Fusion Middleware 10.1.3.5 permet à des attaquants distants dôaffecter la confidentialité via des vecteurs liés à la manipulation de requête HTTP.	15/04/2014	5.0	CVE-2014-0414
oracle -- fusion_middleware	Une vulnérabilité non spécifiée dans les Containers dôOracle pour la composante J2EE dans Oracle Fusion Middleware 10.1.3.5 permet à des attaquants distants dôaffecter lôintégrité via des vecteurs liés à la manipulation des requêtes HTTP, une vulnérabilité différente de celle de CVE-2014-0413	15/04/2014	4.3	CVE-2014-0426
oracle -- sunos	Une vulnérabilité non spécifiée dans Oracle Solaris 9, 10, et 11.1 permet à des utilisateurs locaux dôaffecter la confidentialité, lôintégrité et la disponibilité via des vecteurs inconnus liés à Print Filter Utility.	15/04/2014	4.6	CVE-2014-0442
oracle -- sunos	Une vulnérabilité non spécifiée dans Oracle Solaris 9, 10, et 11.1 permet à des utilisateurs locaux dôaffecter la disponibilité via des vecteurs inconnus liés à Kernel.	15/04/2014	4.9	CVE-2014-0447
oracle -- jdk	Une vulnérabilité non spécifiée dans Oracle Java SE 6u71, 7u51, et 8, et Java SE Embedded 7u51permet à des attaquants distants	15/04/2014	5.0	CVE-2014-0449

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source Info & Correctif
	dôaffecter la confidentialité via des vecteurs inconnus liés à Deployment.			
oracle -- fusion_middleware	Une vulnérabilité non spécifiée dans la composante Oracle WebCenter Portal dans Oracle Fusion Middleware 11.1.1.7 et 11.1.1.8 permet à des attaquants distants dôaffecter la confidentialité via des vecteurs inconnus liés à People Connection.	15/04/2014	5.0	CVE-2014-0450
oracle -- jdk	Une vulnérabilité non spécifiée dans Oracle Java SE 5.0u61, 6u71, 7u51, et 8; JRockit R27.8.1 et R28.3.1; et Java SE Embedded 7u51 permet à des attaquants distants dôaffecter la confidentialité et lôintégrité via des vecteurs inconnus liés à Security.	15/04/2014	4.0	CVE-2014-0453
oracle -- jdk	Une vulnérabilité non spécifiée dans Oracle Java SE 7u51 et 8, et Java SE Embedded 7u51, permet à des attaquants distants dôaffecter la disponibilité via des vecteurs inconnus liés à 2D.	15/04/2014	4.3	CVE-2014-0459
oracle -- jdk	Une vulnérabilité non spécifiée dans Oracle Java SE 5.0u61, 6u71, 7u51, et 8; JRockit R27.8.1 et R28.3.1; et Java SE Embedded 7u51 permet à des attaquants distants dôaffecter la disponibilité et lôintégrité via des vecteurs liés à JNDI.	15/04/2014	5.8	CVE-2014-0460
oracle -- jdk	Une vulnérabilité non spécifiée dans Oracle Java SE 8 permet à des attaquants distants dôaffecter la confidentialité via des vecteurs inconnus liés à Scripting, une vulnérabilité autre que celle de CVE-2014-0464.	15/04/2014	4.3	CVE-2014-0463
oracle -- jdk	Une vulnérabilité non spécifiée dans Oracle Java SE 8 permet à des attaquants distants dôaffecter la confidentialité via des vecteurs inconnus liés à Scripting, une vulnérabilité autre que celle de CVE-2014-0463.	15/04/2014	4.3	CVE-2014-0464
oracle -- fusion_middleware	Une vulnérabilité non spécifiée dans la composante Oracle Endeca Server dans Oracle Fusion Middleware 2.2.2 permet à des attaquants distants dôaffecter lôintégrité via des vecteurs	15/04/2014	4.3	CVE-2014-2399

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source Info & Correctif
	inconnus liés à Oracle Endeca Information Discovery (Anciennement Latitude), une vulnérabilité autre que celle de CVE-2014-2400.			
oracle -- fusion_middleware	Une vulnérabilité non spécifiée dans la composante Oracle Endeca Server dans Oracle Fusion Middleware 2.2.2 permet à des attaquants distants dôaffecter lôintégrité via des vecteurs inconnus liés à Oracle Endeca Information Discovery (Anciennement Latitude), une vulnérabilité autre que celle de CVE-2014-2399.	15/04/2014	4.3	CVE-2014-2400
oracle -- javafx	Une vulnérabilité non spécifiée dans Oracle Java SE 5.0u61, 6u71, 7u51, et 8; JavaFX 2.2.51; et Java SE Embedded 7u51 permet à des attaquants distants dôaffecter la confidentialité via des vecteurs inconnus liés à 2D.	15/04/2014	5.0	CVE-2014-2401
oracle -- jdk	Une vulnérabilité non spécifiée dans Oracle Java SE 6u71, 7u51, et 8, et Java SE Embedded 7u51 permet à des attaquants distants dôaffecter la confidentialité via des vecteurs liés à JAXP.	15/04/2014	5.0	CVE-2014-2403
oracle -- fusion_middleware	Une vulnérabilité non spécifiée dans la composante Oracle Access Manager dans Oracle Fusion Middleware 10.1.4.3, 11.1.1.3.0, 11.1.1.5.0, 11.1.1.7.0, 11.1.2.0.0, 11.1.2.1.0, et 11.1.2.2.0 permet à des utilisateurs authentifiés à distance dôaffecter la confidentialité via des vecteurs inconnus liés à WebGate.	15/04/2014	4.0	CVE-2014-2404
oracle -- fusion_middleware	Une vulnérabilité non spécifiée dans la composante Oracle Data Integrator dans Oracle Fusion Middleware 11.1.1.3.0 permet à des attaquants distants dôaffecter la disponibilité via des vecteurs inconnus liés à Data Quality, une vulnérabilité autre que celle de CVE-2014-2415, CVE-2014-2416, CVE-2014-2417, et CVE-2014-2418	15/04/2014	5.0	CVE-2014-2407
oracle -- database_server	Une vulnérabilité non spécifiée dans la composante Core RDBMS dans Oracle Database Server 11.1.0.7, 11.2.0.3, 11.2.0.4, et 12.1.0.1 permet à des utilisateurs authentifiés à	15/04/2014	6.6	CVE-2014-2408

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source Info & Correctif
	distance dôaffecter la confidentialité et lôintégrité via des vecteurs inconnus liés à "Grant Any Object Privilege."			
oracle -- jdk	Une vulnérabilité non spécifiée dans Oracle Java SE 6u71, 7u51, et 8, et Java SE Embedded 7u51, permet à des attaquants distants dôaffecter la confidentialité et lôintégrité via des vecteurs inconnus liés à Deployment.	15/04/2014	6.4	CVE-2014-2409
oracle -- identity_analytics	Une vulnérabilité non spécifiée dans la composante Oracle Identity Analytics dans Oracle Fusion Middleware, Oracle Identity Analytics 11.1.1.5 et Sun Role Manager 5.0 permet à des utilisateurs authentifiés à distance dôaffecter la confidentialité, lôintégrité et la disponibilité via des vecteurs liés à Security.	15/04/2014	6.5	CVE-2014-2411
oracle -- jdk	Une vulnérabilité non spécifiée dans Oracle Java SE 7u51 et 8, et Java SE Embedded 7u51, permet à des attaquants distants dôaffecter lôintégrité via des vecteurs inconnus liés à Libraries.	15/04/2014	4.3	CVE-2014-2413
oracle -- fusion_middleware	Une vulnérabilité non spécifiée dans la composante Oracle Data Integrator dans Oracle Fusion Middleware 11.1.1.3.0 permet à des attaquants distants dôaffecter la disponibilité via des vecteurs inconnus liés à Data Quality, une vulnérabilité différente de celle de CVE-2014-2407, CVE-2014-2416, CVE-2014-2417, et CVE-2014-2418.	15/04/2014	5.0	CVE-2014-2415
oracle -- fusion_middleware	Une vulnérabilité non spécifiée dans la composante Oracle Data Integrator dans Oracle Fusion Middleware 11.1.1.3.0 permet à des attaquants distants dôaffecter la disponibilité via des vecteurs inconnus liés à Data Quality, une vulnérabilité autre que celle de CVE-2014-2407, CVE-2014-2415, CVE-2014-2417, et CVE-2014-2418	15/04/2014	5.0	CVE-2014-2416
oracle -- fusion_middleware	Une vulnérabilité non spécifiée dans la composante Oracle Data Integrator dans Oracle Fusion Middleware 11.1.1.3.0 permet à des attaquants distants dôaffecter la disponibilité via des vecteurs inconnus liés à Data Quality, une vulnérabilité autre que celle de CVE-2014-2407, CVE-2014-2415, CVE-2014-2416, et CVE-	15/04/2014	5.0	CVE-2014-2417

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source Info & Correctif
	2014-2418			
oracle -- fusion_middleware	Une vulnérabilité non spécifiée dans la composante Oracle Data Integrator dans Oracle Fusion Middleware 11.1.1.3.0 permet à des attaquants distants dôaffecter la disponibilité via des vecteurs inconnus liés à Data Quality, une vulnérabilité autre que celle de CVE-2014-2407, CVE-2014-2415, CVE-2014-2416, et CVE-2014-2417.	15/04/2014	5.0	CVE-2014-2418
oracle -- javafx	Une vulnérabilité non spécifiée dans Oracle Java SE 7u51 et 8, et JavaFX 2.2.51, permet à des attaquants distants dôaffecter la confidentialité, lôintégrité et la disponibilité via des vecteurs inconnus.	15/04/2014	6.8	CVE-2014-2422
oracle -- fusion_middleware	Une vulnérabilité non spécifiée dans la composante Oracle Event Processing dans Oracle Fusion Middleware 11.1.1.7.0 permet à des utilisateurs authentifiés à distance dôaffecter lôintégrité via des vecteurs liés au système CEP.	15/04/2014	4.0	CVE-2014-2424
oracle -- fusion_middleware	Une vulnérabilité non spécifiée dans la composante Oracle OpenSSO dans Oracle Fusion Middleware 8.0 Update 2 Patch 5 permet à des utilisateurs authentifiés à distance dôaffecter la confidentialité via des vecteurs inconnus.	15/04/2014	4.0	CVE-2014-2425
oracle -- fusion_middleware	Une vulnérabilité non spécifiée dans la composante Oracle OpenSSO dans Oracle Fusion Middleware 8.0 Update 2 Patch 5 permet à des utilisateurs authentifiés à distance dôaffecter lôintégrité et la disponibilité via des vecteurs inconnus liés à Admin Console.	15/04/2014	4.9	CVE-2014-2426
oracle -- peoplesoft_products	Une vulnérabilité non spécifiée dans les composantes PeopleSoft Enterprise, CS Campus Self Service dans Oracle PeopleSoft Products 9.0 permet à des utilisateurs authentifiés à distance dôaffecter la confidentialité via des vecteurs inconnus liés à Campus Mobile.	15/04/2014	4.0	CVE-2014-2429

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source Info & Correctif
oracle -- peoplesoft_products	Une vulnérabilité non spécifiée dans les composantes PeopleSoft Enterprise PT PeopleTools dans Oracle PeopleSoft Products 8.53 permet à des attaquants distants dôaffecter la disponibilité via des vecteurs inconnus liés à Integration Broker.	15/04/2014	5.0	CVE-2014-2433
oracle -- mysql	Une vulnérabilité non spécifiée dans Oracle MySQL Server 5.6.15 et antérieurs permet à des utilisateurs authentifiés à distance dôaffecter la disponibilité via des vecteurs liés à DML.	15/04/2014	4.0	CVE-2014-2434
oracle -- mysql	Une vulnérabilité non spécifiée dans Oracle MySQL Server 5.6.16 et antérieurs permet à des utilisateurs authentifiés à distance dôaffecter la disponibilité via des vecteurs inconnus liés à InnoDB.	15/04/2014	4.0	CVE-2014-2435
oracle -- peoplesoft_products	Une vulnérabilité non spécifiée dans les composantes PeopleSoft Enterprise PT PeopleTools dans Oracle PeopleSoft Products 8.52 et 8.53 permet à des attaquants distants dôaffecter la confidentialité via des vecteurs inconnus liés à Integration Broker, une vulnérabilité autre que celle de CVE-2014-2447.	15/04/2014	5.0	CVE-2014-2437
oracle -- virtualization	Une vulnérabilité non spécifiée dans la composante Oracle Secure Global Desktop (SGD) dans Oracle Virtualization 5.0 et 5.1 permet à des attaquants distants dôaffecter la confidentialité et lôintégrité via des vecteurs inconnus liés à Workspace Web Application.	15/04/2014	6.4	CVE-2014-2439
oracle -- vm_virtualbox	Une vulnérabilité non spécifiée dans la composante Oracle VM VirtualBox dans Oracle Virtualization VirtualBox avant 4.1.32, 4.2.24, et 4.3.10 permet à des utilisateurs locaux dôaffecter la confidentialité, lôintégrité et la disponibilité via des vecteurs liés à Graphics driver (WDDM) pour des hôtes Windows.	15/04/2014	4.4	CVE-2014-2441
oracle -- mysql	Une vulnérabilité non spécifiée dans Oracle MySQL Server 5.6.15 et antérieurs permet à des utilisateurs authentifiés à distance dôaffecter la disponibilité via des vecteurs liés à MyISAM.	15/04/2014	4.0	CVE-2014-2442

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source Info & Correctif
oracle -- peoplesoft_products	Une vulnérabilité non spécifiée dans la composante PeopleSoft Enterprise PT PeopleTools dans Oracle PeopleSoft Products 8.52 et 8.53 permet à des attaquants distants dôaffecter lôintégrité via des vecteurs liés à PIA Core Technology.	15/04/2014	4.3	CVE-2014-2443
oracle -- mysql	Une vulnérabilité non spécifiée dans Oracle MySQL Server 5.6.15 et antérieurs permet à des utilisateurs authentifiés à distance dôaffecter la confidentialité, lôintégrité et la dsponibilité via des vecteurs liés à InnoDB.	15/04/2014	6.5	CVE-2014-2444
oracle -- peoplesoft_products	Une vulnérabilité non spécifiée dans la composante PeopleSoft Enterprise PT PeopleTools dans Oracle PeopleSoft Products 8.52 et 8.53 permet à des utilisateurs authentifiés à distance dôaffecter la confidentialité via des vecteurs liés à QAS.	15/04/2014	4.0	CVE-2014-2446
oracle -- peoplesoft_products	Une vulnérabilité non spécifiée dans la composante PeopleSoft Enterprise PT PeopleTools dans Oracle PeopleSoft Products 8.52 et 8.53 permet à des attaquants distants dôaffecter la confidentialité via des vecteurs inconnus liés à Integration Broker, une vulnérabilité différente de celle de CVE-2014-2437.	15/04/2014	5.0	CVE-2014-2447
oracle -- peoplesoft_products	Une vulnérabilité non spécifiée dans la composante PeopleSoft Enterprise PT PeopleTools dans Oracle PeopleSoft Products 8.52 et 8.53 permet à des attaquants distants dôaffecter la confidentialité via des vecteurs inconnus liés à Install and Packaging.	15/04/2014	5.0	CVE-2014-2448
oracle -- peoplesoft_products	Une vulnérabilité non spécifiée dans la composante PeopleSoft Enterprise HRMS Talent Acquisition Manager dans Oracle PeopleSoft Products 9.0, 9.1, et 9.2 permet à des utilisateurs authentifiés à distance dôaffecter la confidentialité via des vecteurs inconnus liés à Security.	15/04/2014	4.0	CVE-2014-2449
oracle -- mysql	Une vulnérabilité non spécifiée dans Oracle MySQL Server 5.6.15 et antérieurs permet à des utilisateurs authentifiés à distance dôaffecter la disponibilité via des vecteurs inconnus liés à Optimizer.	15/04/2014	4.0	CVE-2014-2450

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source Info & Correctif
oracle -- fusion_middleware	Une vulnérabilité non spécifiée dans la composante Oracle Access Manager dans Oracle Fusion Middleware 11.1.1.5 permet à des utilisateurs authentifiés à distance dôaffecter la disponibilité via des vecteurs inconnus liés à Webserver Plugin.	15/04/2014	4.0	CVE-2014-2452
oracle -- hyperion	Une vulnérabilité non spécifiée dans la composante Hyperion Common Admin dans Oracle Hyperion 11.1.2.2 et 11.1.2.3 permet à des attaquants distants dôaffecter lôintégrité via des vecteurs inconnus liés à User Interface.	15/04/2014	4.3	CVE-2014-2453
oracle -- hyperion	Une vulnérabilité non spécifiée dans la composante Hyperion Common Admin dans Oracle Hyperion 11.1.2.2 et 11.1.2.3 permet à des attaquants distants dôaffecter la confidentialité via des vecteurs inconnus liés à User Interface.	15/04/2014	4.3	CVE-2014-2454
oracle -- hyperion	Une vulnérabilité non spécifiée dans la composante Hyperion Common Admin dans Oracle Hyperion 11.1.2.2 et 11.1.2.3 permet à des utilisateurs authentifiés à distance dôaffecter l confidentialité, lôintégrité et la disponibilité via des vecteurs inconnus liés à User Interface.	15/04/2014	6.0	CVE-2014-2455
oracle -- supply_chain_products_suite	Une vulnérabilité non spécifiée dans la composante Oracle Agile Product Lifecycle dans Oracle Supply Chain Products Suite 6.0 et 6.1.0 permet à des attaquants distants dôaffecter lôintégrité via des vecteurs inconnus liés à Install.	15/04/2014	4.3	CVE-2014-2457
oracle -- supply_chain_products_suite	Une vulnérabilité non spécifiée dans la composante Oracle Agile Product Lifecycle dans Oracle Supply Chain Products Suite 6.1.0.3 et 6.1.1.3 permet à des attaquants distants dôaffecter lôintégrité vias des vecteurs inconnus liés à Install.	15/04/2014	4.3	CVE-2014-2458
oracle -- supply_chain_products_suite	Une vulnérabilité non spécifiée dans la composante Oracle Transportation Management dans Oracle Supply Chain Products Suite 5.5.06, 6.0, 6.1, 6.2, 6.3, 6.3.1, 6.3.2, et 6.3.3 permet à des utilisateurs uathentifiés à distance dôaffecter la confidentialité via des vecteurs liés à CSV Management.	15/04/2014	4.0	CVE-2014-2460

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source Info & Correctif
oracle -- supply_chain_products_suite	Une vulnérabilité non spécifiée dans la composante Oracle Transportation Management dans Oracle Supply Chain Products Suite 5.5.06, 6.0, 6.1, 6.2, 6.3, 6.3.1, 6.3.2, et 6.3.3 permet à des attaquants distants dôaffecter la confidentialité via des vecteurs inconnus liés à Security.	15/04/2014	5.0	CVE-2014-2461
oracle -- virtualization	Une vulnérabilité non spécifiée dans la composante Oracle Secure Global Desktop (SGD) dans Oracle Virtualization 4.63, 4.71, 5.0, et 5.1 permet à des attaquants distants dôaffecter lôintégrité via des vecteurs inconnus liés à Workspace Web Application.	15/04/2014	4.3	CVE-2014-2463
oracle -- supply_chain_products_suite	Une vulnérabilité non spécifiée dans la composante Oracle Agile PLM Framework dans Oracle Supply Chain Products Suite 9.3.3 permet à des attaquants distants dôaffecter lôintégrité via des vecteurs inconnus liés à Security.	15/04/2014	4.3	CVE-2014-2465
oracle -- siebel_crm	Une vulnérabilité non spécifiée dans la composante Siebel UI Framework dans Oracle Siebel CRM 8.1.1 et 8.2.2 permet à des attaquants distants dôaffecter lôintégrité via des vecteurs liés à Open_UI.	15/04/2014	4.3	CVE-2014-2468
oracle -- sunos	Une vulnérabilité non spécifiée dans Lighthttpd dans Oracle Solaris 11.1 permet à des attaquants distants de provoquer un déni de service via des vecteurs inconnus.	17/04/2014	5.0	CVE-2014-2469
oracle -- ilearning	Une vulnérabilité non spécifiée dans la composante Oracle iLearning dans Oracle iLearning 6.0 et 6.1 permet à des attaquants distants dôaffecter lôintégrité via des vecteurs inconnus liés à Learner Pages.	15/04/2014	4.3	CVE-2014-2471
oracle -- identity_manager	Une vulnérabilité Open redirect dans Oracle Identity Manager 11g R2 SP1 (11.1.2.1.0) permet à des attaquants distants de rediriger les utilisateurs vers des sites web arbitraires et mener à des attaques par hameçonnage via une URL dans le parmaètre backUrl dans une action changepwd vers identity/faces/firstlogin.	17/04/2014	5.8	CVE-2014-2880

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source Info & Correctif
osisoft -- pi_interface	Le pilote DNP Master dans lôinterface OSIsoft PI avant 3.1.2.54 pour DNP3 permet à des attaquants physiquement proches de provoquer un déni de service (extinction dôinterface) via une entrée trafiquée sur une liaison série.	12/04/2014	4.7	CVE-2013-2828
paperthin -- commonspot_content_server	De nombreuses vulnérabilités cross-site scripting (XSS) dans PaperThin CommonSpot avant 7.0.2 et 8.x avant 8.0.3 permettent à des attaquants distants dôinjecter un script web ou HTML arbitraire via une requête http falsifiée vers une composante (1) ColdFusion ou (2) JavaScript.	15/04/2014	4.3	CVE-2014-2860
paperthin -- commonspot_content_server	Une vulnérabilité Incomplete blacklist dans PaperThin CommonSpot avant 7.0.2 et 8.x avant 8.0.3 permet à des attaquants distants de mener des attaques cross-site scripting (XSS) via des chaines de caractères fabriqués, comme démontré par le contournement dôun mécanisme de protection qui enlève uniquement la chaine de caractère « alert ».	15/04/2014	4.3	CVE-2014-2861
paperthin -- commonspot_content_server	PaperThin CommonSpot avant 7.0.2 et 8.x avant 8.0.3 ne vérifie lôautorisation dans des situations non spécifiées, ce qui permet à des utilisateurs authentifiées à distance de réaliser des actions via des vecteurs inconnus.	15/04/2014	6.5	CVE-2014-2862
paperthin -- commonspot_content_server	PaperThin CommonSpot avant 7.0.2 et 8.x avant 8.0.3 permet à des attaquants distants dôobtenir des informations sensibles via des requêtes vers des URIs non spécifiées, comme démontré par les informations nom de chemin, server SQL, adresse e-mail et adresse IP.	15/04/2014	5.0	CVE-2014-2869
paperthin -- commonspot_content_server	La configuration par défaut de PaperThin CommonSpot avant 7.0.2 et 8.x avant 8.0.3 utilise des textes en clair pour le stockage des informations dôauthentification dans une base de données, ce qui rend plus facile pour des attaquants selon le contexte dôobtenir des informations sensibles via des vecteurs non spécifiés.	15/04/2014	5.0	CVE-2014-2870

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source Info & Correctif
paperthin -- commonspot_content_server	PaperThin CommonSpot avant7.0.2 et 8.x avant 8.0.3 se fie une session HTTP pour entrer les informations dôauthentification sur des pages de login, ce qui permet à des attaquants distants dôobtenir des informations sensibles en réniflant le réseau.	15/04/2014	5.0	CVE-2014-2871
paperthin -- commonspot_content_server	PaperThin CommonSpot avant7.0.2 et 8.x avant 8.0.3 permet à des attaquants distants dôobtenir potentiellement des informations sensibles à partir de listing de répertoire via des vecteurs non spécifiés.	15/04/2014	5.0	CVE-2014-2872
paperthin -- commonspot_content_server	PaperThin CommonSpot avant7.0.2 et 8.x avant 8.0.3 ne requière pas une authentification pour lôaccès aux fichiers log, ce qui permet à des attaquants distants dôobtenir des informations sensibles sur le serveur en utilisant un nom prédictible dans une requête dôun fichier.	15/04/2014	5.0	CVE-2014-2873
python -- pillow	Les fonctions (1) load_djpeg dans JpegImagePlugin.py, (2) Ghostscript dans EpsImagePlugin.py, (3) load dans IptcImagePlugin.py, and (4) _copy dans Image.py in Python Image Library (PIL) 1.1.7 et antérieurs et Pillow avant 2.3.1 ne créent pas correctement les fichiers temporaires, ce qui permet à des utilisateurs locaux dôécraser des fichiers arbitraires et obtenir des informations sensibles via une attaque symlink sur un fichier temporaire.	17/04/2014	4.4	CVE-2014-1932
raoul_proenca -- gnew	De nombreuses vulnérabilités cross-site scripting (XSS) dans Gnew 2013.1 permettent à des attaquants distants dôinjecter un script web ou HTML arbitraire via le paramètre gnew_template vers (1) users/profile.php, (2) articles/index.php, ou (3) admin/polls.php; (4) le paramètre category_id vers news/submit.php; le paramètre news_id vers (5) news/send.php ou (6) comments/add.php; ou (7) le paramètre post_subject ou (8) le paramètre thread_id vers posts/edit.php.	15/04/2014	4.3	CVE-2013-7368
redhat -- network_proxy	Lôaffichage du monitoring de la sonde dans spacewalk-java avant 2.1.148-1 et Red Hat Network (RHN) Satellite 4.0.0 à	15/04/2014	6.0	CVE-2010-2236

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source Info & Correctif
	4.2.0 et 5.1.0 à 5.3.0, et Proxy 5.3.0, permet à des utilisateurs authentifiés à distance avec des permissions dôadministrer les sondes de monitoring, dôexécuter un code arbitraire via des vecteurs non spécifiés, liés à backticks.			
redhat -- libvirt	Le pilote LXC (lxc/lxc_driver.c) dans libvirt 1.0.1 à 1.2.1 permet à des utilisateurs locaux de (1) supprimer des appareils hôtes arbitraires via lôAPI virDomainDeviceDettach et une attaque symlink sur /dev dans le container ; (2) créer des nî uds arbitraires (mknod) via lôAPI virDomainDeviceAttach et une attaque symlink sur /dev dans le container ; et provoquer un déni de service (extinction ou redémarrage de lôOS de lôhôte) via les API (3) virDomainShutdown ou (4) virDomainReboot et une attaque symlink sur /dev/initctl dans le container lié à « au chemin sous /proc/$PID/root » et la fonction virInitctlSetRunLevel.	15/04/2014	5.8	CVE-2013-6456
redhat -- openstack	PackStack dans Red Hat OpenStack 4.0 nôapplique pas les groupes de sécurité par défaut lorsquôil est déployé vers Neutron, ce qui permet à des attaquants distants de contourner les restrictions dôaccès prévues et réaliser des connexions non autorisées.	17/04/2014	6.4	CVE-2014-0071
redmine -- redmine	Une vulnérabilité Open redirect dans la fonction redirect_back_or_default dans app/controllers/application_controller.rb dans Redmine avant 2.4.5 et 2.5.x avant 2.5.1 permet à des attaquants distants de rédiriger des utilisateurs vers des sites web arbitraires et mener à des attaques par hameçonnage via une URL dans lôURL arrière (paramètre back_url).	11/04/2014	5.8	CVE-2014-1985
reviewboard -- review_board	Une vulnérabilité Cross-site scripting (XSS) dans la liste Submitters dans Review Board 1.6.x avant 1.6.18 et 1.7.x avant 1.7.12 permet à des attaquants distants dôinjecter un scrip web ou HTML arbitraire via le nom complet dôun utilisateur.	11/04/2014	4.3	CVE-2013-4795

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source Info & Correctif
rodrigo_polo -- stream_video_player	Une vulnérabilité Cross-site request forgery (CSRF) dans le plugin Stream Video Player 1.4.0 pour WordPress permet à des attaquants distants de détourner lôauthentification des administrateurs pour des requêtes qui changent les configurations du plugin via des vecteurs non spécifiés.	11/04/2014	6.8	CVE-2013-2706
roundup-tracker -- roundup	Une vulnérabilité Cross-site scripting (XSS) dans lôaffichage de lôhistorique dans Roundup avant 1.4.20 permet à des attaquants distants dôinjecter un scrip web ou HTML arbitraire via un nom dôutilisateur, en relation avec la génération dôun lien.	11/04/2014	4.3	CVE-2012-6130
roundup-tracker -- roundup	Une vulnérabilité Cross-site scripting (XSS) dans cgi/client.py dans Roundup avant 1.4.20 permet à des attaquants distants dôinjecter un script web ou HTML arbitraire via le paramètre @action vers support/issue1.	11/04/2014	4.3	CVE-2012-6131
sap -- router	La fonction passwordCheck dans SAP Router 721 patch 117, 720 patch 411, 710 patch 029 et antérieurs termine la validation de lôentrée dôun mot de passe dans Route Permission Table lorsquôil rencontre un premier caractère incorrect, ce qui permet à des attaquants distants dôobtenir des mots de passe via une attaque brute-force qui se base sur les différences de synchronisation dans les réponses aux mots de passe dévinés et incorrects, aussi connu sous lôappelation dôattaque de synchronisation de canal-latéral.	17/04/2014	4.3	CVE-2014-0984
snilesh -- content_slide	Une vulnérabilité Cross-site request forgery (CSRF) dans le plugin Content Slide 1.4.2 pour WordPress permet à des attaquants distants de détourner lôauthentification des administrateurs pour des requêtes qui changent les configurations du plugin via des vecteurs non spécifiés.	11/04/2014	6.8	CVE-2013-2708
springsource -- spring_framework	Jaxb2RootElementHttpMessageConverter dans Spring MVC dans Spring Framework avant 3.2.8 et 4.0.0 avant 4.0.2 ne désactive pas la résolution de lôentité externe, ce qui permet à des attaquants distants de lire des fichiers arbitraires, provquer un	17/04/2014	6.8	CVE-2014-0054

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source Info & Correctif
	déni de service et mener à des attaques CSRF via des XML trafiqués, aussi connue sous lâappelation problème de lâEntité XML externe (XXE). REMARQUE : cette vulnérabilité existe à cause dâune résolution imcomplète pour CVE-2013-4152, CVE-2013-7315, et CVE-2013-6429.			
squid-cache -- squid	Squid 3.1 avant 3.3.12 et 3.4 avant 3.4.4, lorsque SSL-Bump est activé, permet à des attaquants distants de provoquer un déni de service (échec dâassertion) via une requête trafiquée sur un intervalle, en relation avec la gestion du status.	14/04/2014	5.0	CVE-2014-0128
strongswan -- strongswan	IKEv2 dans strongSwan 4.0.7 avant 5.1.3 permet à des attaquants distants de contourner lâauthentification en retapant un IKE_SA pendant (1) une initialisation ou (2) une réauthentification, ce qui déclenche le passage du status de IKE_SA à établi.	16/04/2014	6.4	CVE-2014-2338
sun -- sunos	Une vulnérabilité non spécifiée dans Oracle Solaris 10, lorsquâil est exécuté sur une plateforme SPARC64-X, permet à des utilisateurs locaux dâaffecter la confidentialité, lâintégrité et la disponibilité via des vecteurs inconnus.	15/04/2014	4.6	CVE-2014-0421
suse -- studio_extension_for_system_z	Une vulnérabilité Cross-site scripting (XSS) dans lâonglet des fichiers superposés dans SUSE Studio Extension pour System z 1.2 avant 1.2.1 permet à des attaquants distants dâinjecter un script web ou HTML arbitraire via une application trafiquée, en relation avec le clonage.	16/04/2014	4.3	CVE-2011-4193
tenable -- nessus	Une condition de compétition dans le plugin wmi_malware_scan.nbin avant 201402262215 pour Nessus 5.2.1 permet à des utilisateurs locaux dâobtenir des privilèges en remplaçant lâexécutable de lâagent soluble dans le répertoire temporaire de Windows avec un programme Cheval de Troyes.	11/04/2014	6.9	CVE-2014-2848
vmware -- vsphere_client	VMware vSphere Client 5.0 avant Update 3 et 5.1 avant Update 2 ne valide pas correctement les certificats X.509, ce qui permet à des attaquants man-in-the-middle dâusurper des serveurs SSL via un certificat falsifié.	11/04/2014	5.8	CVE-2014-1210

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source Info & Correctif
vmware -- player	vmx86.sys dans VMware Workstation 10.0.1 build 1379776 et VMware Player 6.0.1 build 1379776 sur Windows pourrait permettre à des utilisateurs locaux de provoquer un déni de service (violation de lôaccès en lecture et crash système) via un tampon trafiqué dans un appel IOCTL. REMARQUE : le chercheur rapporte « le fabricant a décrit le problème comme non-exploitable »	15/04/2014	4.9	CVE-2014-2384
xen -- xen	Le pilote netback dans Xen, lorsquôil utilise certaines versions de Linux qui ne permettent pas la mise en veille dans un contexte softirq, permet à des administrateurs locaux de la machine hôte de provoquer un déni de service (erreur "scheduling while atomic" et crash de lôhôte) via un paquet malformé qui provoque un mutex dôêtre prix lorsquôon essaie de désactiver lôinterface.	15/04/2014	4.4	CVE-2014-2580
zyxel -- n300_netusb_nbg-419n	Le routeur ZyXEL Wireless N300 NetUSB NBG-419N doté du firmware 1.00(BFQ.6)C0 permet à des attaquants distants de contourner lôauthentification en utilisant des séquences %2F en lieu et place des caractères / (slash).	15/04/2014	6.1	CVE-2014-0353

Retour haut de page

Vulnérabilités mineures

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source Info & Correctif
apache -- zookeeper	Apache Zookeeper journalise en texte clair les mots de passe admin, ce qui permet à des utilisateurs locaux dôobtenir des informations sensibles en lisant les logs.	17/04/2014	2.1	CVE-2014-0085
canonical -- update-manager	DistUpgrade/DistUpgradeViewKDE.py dans Update Manager avant 1:0.87.31.1, 1:0.134.x avant 1:0.134.11.1, 1:0.142.x avant 1:0.142.23.1, 1:0.150.x avant 1:0.150.5.1, et 1:0.152.x avant 1:0.152.25.5 ne crée pas correctement les	17/04/2014	1.9	CVE-2011-3154

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source Info & Correctif
	fichiers temporaires, ce qui permet à des utilisateurs locaux dôobtenir le contenu du fichier XAUTHORITY pour un utilisateur via une attaque symlink sur un fichier temporaire.			
canonical -- accountsservice	Le package Ubuntu AccountsService avant 0.6.14-1git1ubuntu1.1 nôabandonne pas correctement les privilèges lorsquôil change les configurations de la langue, ce qui permet à des utilisateurs locaux de modifier des fichiers arbitraires via des vecteurs non spécifiés.	16/04/2014	3.6	CVE-2011-4406
citrix -- vdi-in-a-box	Citrix VDI-in-a-Box 5.3.x avant 5.3.6 et 5.4.x avant 5.4.3 permet à des utilisateurs locaux dôobtenir des informations dôauthentification de lôadministrateur en lisant les logs.	15/04/2014	2.1	CVE-2014-2690
hp -- array_configuration_utility	Une vulnérabilité non spécifiée dans HP Array Configuration Utility, Array Diagnostics Utility, ProLiant Array Diagnostics, et SmartSSD Wear Gauge Utility 9.40 et antérieurs permet à des utilisateurs locaux dôobtenir des privilèges via des vecteurs inconnus.	12/04/2014	2.1	CVE-2013-6216
marcel_brinkkemper -- lazyest-gallery	Une vulnérabilité Cross-site scripting (XSS) dans le plugin Lazyest Gallery avant 1.1.21 pour WordPress permet à des attaquants distants dôinjecter un script web ou HTML arbitraire via un tag EXIF. REMARQUE : certains des détails sont disponibles auprès des sources dôinformation dôune tierce partie.	11/04/2014	2.6	CVE-2014-2333
mysql -- mysql	Une vulnérabilité non spécifiée dans Oracle MySQL Server 5.5.36 et antérieurs et 5.6.16 et antérieurs permet à des utilisateurs authentifiés à distance dôaffecter la disponibilité via des vecteurs inconnus liés à Performance Schema.	15/04/2014	3.5	CVE-2014-2430
mysql -- mysql	Une vulnérabilité non spécifiée dans Oracle MySQL Server 5.5.36 et antérieurs et 5.6.16 et antérieurs permet à des attaquants distants dôaffecter la disponibilité via des vecteurs inconnus liés à Options.	15/04/2014	2.6	CVE-2014-2431

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source Info & Correctif
mysql -- mysql	Une vulnérabilité non spécifiée dans la composante Oracle MySQL Server 5.5.35 et antérieurs et 5.6.15 et antérieurs permet à des utilisateurs authentifiés à distance dôaffecter la disponibilité via des vecteurs inconnus liés à Federated.	15/04/2014	2.8	CVE-2014-2432
mysql -- mysql	Une vulnérabilité non spécifiée dans Oracle MySQL Server 5.5.35 et antérieurs et 5.6.15 et antérieurs permet à des attaquants distants dôaffecter la disponibilité via des vecteurs inconnus liés à Replication	15/04/2014	3.5	CVE-2014-2438
novell -- suse_lifecycle_management_server	SUSE Lifecycle Management Server avant 1.1 utilises des informations dôauthentification postgres universellement lisibles, ce qui permet à des utilisateurs locaux dôobtenir des informations sensibles via des vecteurs non spécifiés.	16/04/2014	2.1	CVE-2011-0993
ontariosystems -- artiva_architect	Lôimplémentation de Artiva Agency Single Sign-On (SSO) dans Artiva Workstation 1.3.x avant 1.3.9, Artiva Rm 3.1 MR7, Artiva Healthcare 5.2 MR5, et Artiva Architect 3.2 MR5, lorsque lôoption domain-name est activée, permet à des attaquants distants de se logguer arbitrairement aux comptes de domaine en utlisant le nom dôutilisateur correspondant sur une machine client Windows.	15/04/2014	3.5	CVE-2014-0348
oracle -- fusion_middleware	Une vulnérabilité non spécifiée dans la composante Oracle OpenSSO dans Oracle Fusion Middleware 8.0 Update 2 Patch 5 permet à des utilisateurs authentifiés à distance dôaffecter lôintégrité via des vecteurs inconnus liés à Admin Console.	15/04/2014	3.5	CVE-2014-0465
oracle -- javafx	Une vulnérabilité non spécifiée dans Oracle Java SE 5.0u61, 6u71, 7u51, et 8; JavaFX 2.2.51; et JRockit R27.8.1 et R28.3.1 permet à des utilisateurs authentifiés à distance dôaffecter lôintégrité via des vecteurs inconnus liés à Javadoc.	15/04/2014	3.5	CVE-2014-2398
oracle -- jdk	Une vulnérabilité non spécifiée dans Oracle Java SE 6u71, 7u51, et 8, et Java SE Embedded 7u51, permet à des attaquants distants dôaffecter lôintégrité via des vecteurs inconnus liés à Deployment.	15/04/2014	2.6	CVE-2014-2420

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source Info & Correctif
oracle -- supply_chain_products_suite	Une vulnérabilité non spécifiée dans la composante Oracle Agile PLM Framework dans Oracle Supply Chain Products Suite 9.3.3 permet à des utilisateurs authentifiés à distance dôaffecter lôintégrité via des vecteurs inconnus liés à Security, une vulnérabilité différente de celle de CVE-2014-2467.	15/04/2014	3.5	CVE-2014-2445
oracle -- mysql	Une vulnérabilité non spécifiée dans Oracle MySQL Server 5.6.15 et antérieures permet à des utilisateurs authentifiés à distance dôaffecter la disponibilité via des vecteurs inconnus liés à Privileges.	15/04/2014	3.5	CVE-2014-2451
oracle -- supply_chain_products_suite	Une vulnérabilité non spécifiée dans la composante Oracle Transportation Management dans Oracle Supply Chain Products Suite 6.3.2 et 6.3.3 permet à des utilisateurs locaux dôaffecter la confidentialité, lôintégrité et la disponibilité via des vecteurs inconnus liés à Security.	15/04/2014	3.7	CVE-2014-2459
oracle -- supply_chain_products_suite	Une vulnérabilité non spécifiée dans la composante Oracle Agile PLM Framework dans Oracle Supply Chain Products Suite 9.3.3.0 permet à des utilisateurs authentifiés à distance dôaffecter la confidentialité via des vecteurs inconnus liés à Security.	15/04/2014	3.5	CVE-2014-2464
oracle -- supply_chain_products_suite	Une vulnérabilité non spécifiée dans la composante Oracle Agile PLM Framework dans Oracle Supply Chain Products Suite 9.3.3 permet à des utilisateurs authentifiés à distance dôaffecter la confidentialité via des vecteurs inconnus liés à Security.	15/04/2014	2.1	CVE-2014-2466
oracle -- supply_chain_products_suite	Une vulnérabilité non spécifiée dans la composante Oracle Agile PLM Framework dans Oracle Supply Chain Products Suite 9.3.3 permet à des utilisateurs authentifiés à distance dôaffecter lôintégrité via des vecteurs inconnués liés à Security, une vulnérabilité différente de celle de CVE-2014-2445.	15/04/2014	3.5	CVE-2014-2467

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source Info & Correctif
packagekit_project -- packagekit	Le backend Zypper (aussi connu sous ZYpp) dans PackageKit avant 0.8.8 permet aux utilisateurs locaux de rétrograder des paquets via la méthode "install updates".	16/04/2014	2.1	CVE-2013-1764
pivotx -- pivotx	De nombreuses vulnérabilités cross-site scripting (XSS) dans PivotX avant 2.3.9 permettent à des utilisateurs authentifiés à distance dôinjecter un script web ou HTML via le champ title vers (1) templates_internal/pages.tpl, (2) templates_internal/home.tpl, ou (3) templates_internal/entries.tpl; (4) un champ event vers objects.php; ou le champ (5) email ou (6) nickname vers pages.php, liés à templates_internal/users.tpl.	15/04/2014	3.5	CVE-2014-0341
python -- pillow	Les scripts (1) JpegImagePlugin.py et (2) EpsImagePlugin.py dans Python Image Library (PIL) 1.1.7 et antérieurs et Pillow avant 2.3.1 utilises les noms des fichiers temporaires dans la ligne de commande, ce qui rend plus facile à des utilisateurs locaux de mener des attaques symlink en listant les processus.	17/04/2014	2.1	CVE-2014-1933
websense -- triton_unified_security_center	Le module Settings dans Websense Triton Unified Security Center 7.7.3 avant Hotfix 31, Web Filter 7.7.3 avant Hotfix 31, Web Security 7.7.3 avant Hotfix 31, Web Security Gateway 7.7.3 avant Hotfix 31, et Web Security Gateway Anywhere 7.7.3 avant Hotfix 31 permet à des utilisateurs authentifiés à distance de lire des mots de passe en texte clair en remplaçant type="password" avec type="text" dans un élément INPUT dans la composante (1) Log Database ou (2) User Directories	12/04/2014	3.5	CVE-2014-0347

Retour haut de page

Computer Incidents Response Team (CIRT)
01 BP 6437 Ouagadougou 01
Tel : +226 50 37 53 60/61/62 Poste 262 ï Fax : +226 50 37 53 64 ï Email : cirt@cirt.bf ï Web : http://www.cirt.bf