CENTRE DE CYBERSÉCURITÉ DU BURKINA FASO
Notre objectif est de réduire la vulnérabilité du cyberespace, de gérer les incidents de sécurité informatique et de renforcer la culture de cybersécurité

Bulletin hebdomadaire des vulnérabilités n°BV14-02

Date de publication : 31/03/2014

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 s'agit de celles ayant un score CVSS compris entre 7.0 et 10
- Les **Vulnérabilités majeures** : il s'agit de celles ayant un score CVSS compris entre 4.0 et 6.9
- Les **Vulnérabilités mineures** : il s'agit 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'**éditeur 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 d'avoir 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 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 d'information et des processus automatisés.

Vulnérabilités critiques

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source d'information & de correctif
alliedtelesis -- at-rg634a	L'interface d'administration du routeur ADSL large-band AT-RG634A 3.3+, iMG624A avec le firmware 3.5, iMG616LH avec le firmware 2.4, et iMG646BD avec le firmware 3.5 de Allied Telesis, permet à des attaquants distants d'obtenir des privilèges et exécuter des commandes arbitraires via une requête directe à cli.html.	31/03/2014	10.0	CVE-2014-1982

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source dôinformation & de correctif
androidsu -- chainsdd_superuser	Une vulnérabilité de chemin de recherche non fiable dans le paquet ChainsDD Superuser 3.1.3 pour Android 4.2.x et antérieures, CyanogenMod/ClockWorkMod/Koush Superuser 1.0.2.1 pour Android 4.2.x et antérieures et Chainfire SuperSU avant 1.69 pour Android 4.2.x et antérieures, permet à des attaquants de charger un fichier .jar arbitraire et obtenir des privilèges via une variable dôenvironnement BOOTCLASSPATH falsifiée pour un processus /system/xbin/su. REMARQUE : un autre chercheur était incapable de reproduire cela avec ChainsDD Superuser.	31/03/2014	10.0	CVE-2013-6774
autodesk -- sketchbook	Un dépassement de tas dans Autodesk SketchBook pour Enterprise 2014, Pro et Express avant 6.25 et Copic Edition avant 2.0.2 permet à un attaquant distant dôexécuter un code arbitraire via des données dôun canal RLE-compressé se trouvant dans un fichier PSD.	02/04/2014	9.3	CVE-2013-5365
ca -- erwin_web_portal	De nombreuses vulnérabilités « traversée de chemins » dans CA ERwin Web Portal 9.5 permettent à des attaquants distants dôobtenir des informations sensibles, de contourner des restrictions dôaccès prévues, de causer un déni de service, ou éventuellement dôexécuter un code arbitraire via des vecteurs non spécifiés.	04/04/2014	7.5	CVE-2014-2210
cartpauj -- mingle-forum	De nombreuses vulnérabilités « injections SQL » dans wpf.class.php dans le plugin du Forum Mingle avant 1.0.34 pour WordPress permettent à des attaquants distants dôexécuter des commandes SQL arbitraires via le numéro (id) du paramètre dans une action (1) remove_post, (2) sticky, ou (3) closed de viewtopic ou (4) le paramètre thread dans une action postreply vers index.php	02/04/2014	7.5	CVE-2013-0735
chainfire -- supersu	Le paquet Chainfire SuperSU avant 1.69 pour Android permet à des attaquants dôobtenir des privilèges via les types de metacaractères (1) backtick ou (2) $() du shell dans lôoption ï c vers /system/xbin/su.	31/03/2014	10.0	CVE-2013-6775
checkpoint -- security_gateway	De nombreuses vulnérabilités non spécifiées dans Check Point Security Gateway 80 R71.x avant R71.45 (730159141) et R75.20.x avant R75.20.4 et les appareils 600 et1100 R75.20.x avant R75.20.42 ont un impact inconnu et des vecteurs dôattaques relatifs à « dôimportantes corrections de sécurité »	01/04/2014	10.0	CVE-2013-7350

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source dôinformation & de correctif
coreftp -- core_ftp	Un dépassement de pile dans Core FTP avant 2.2 build 1785 permet à des serveurs FTP distants dôexécuter un code arbitraire via un nom de chemin falsifié dans une commande réponse CWD.	04/04/2014	9.3	CVE-2013-3930
crowbar -- barclamp	Barclamp (alias barclamp-network) 1.7 pour Crowbar Framework tel quôutilisé dans SUSE Cloud 3 nâactive pas netfilter sur les ponts (bridges) lorsque de nouvelles instances sont créées, ce qui permet à des attaquants distants de contourner les restrictions de sécurité de groupe via des vecteurs non spécifiés relatifs aux adresses IP flottantes.	04/04/2014	7.5	CVE-2014-0592
emc -- vplex_geosynchrony	Une vulnérabilité « traversée de répertoire » dans EMC VPLEX GeoSynchrony 4.x et 5.x avant 5.3 permet à des utilisateurs authentifiés à distance dôexécuter un code arbitraire via des vecteurs non spécifiés.	01/04/2014	9.0	CVE-2014-0632
emc -- vplex_geosynchrony	Lôinterface graphique utilisateur dans EMC VPLEX GeoSynchrony 4.x et 5.x avant 5.3 ne valide pas correctement les valeurs dôexpiration des sessions, ce qui pourrait rendre plus simple pour des attaquants distants dôexécuter un code arbitraire en prenant appui sur une station de travail sans surveillance.	01/04/2014	7.7	CVE-2014-0633
emc -- vplex_geosynchrony	Une vulnérabilité de fixation de session dans EMC VPLEX GeoSynchrony 4.x et 5.x avant 5.3 permet à des attaquants distants de détourner des sessions web via des vecteurs non spécifiés.	01/04/2014	7.5	CVE-2014-0635
horde -- horde_application_framework	Le script framework/Util/lib/Horde/Variables.php dans la bibliothèque Util dans Horde avant 5.1.1 permet à des attaquants distants de mener des attaques par injection dôobjet et exécuter un code PHP arbitraire via un faux objet sérialisé dans le formulaire _formvars.	01/04/2014	7.5	CVE-2014-1691
hp -- storeonce_2610_iscsi_backup_system	Une vulnérabilité non spécifiée dans HP StoreOnce Virtual Storage Appliance (VSA) avant 3.7.2, StoreOnce 27xx et 4210iSCSI Backup System avant 3.9.0, StoreOnce 4210 FC Backup System avant 3.9.0 et StoreOnce 4xxx Backup System avant 3.9.0 permet à des attaquants distants dôobtenir des informations sensibles ou causer un déni de service via des vecteurs inconnus.	28/03/2014	7.8	CVE-2013-6211
ibm -- flex_system_v7000_software	IBM SAN Volume Controller; Storwize V3500, V3700, V5000 et V7000; et Flex System V7000 versions 6.3 et 6.4 avant 6.4.1.8, 7.1 et 7.2 avant 7.2.0.3, permettent à des attaquants distants dôobtenir un accès en ligne de	28/03/2014	7.5	CVE-2014-0880

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source dôinformation & de correctif
	commande et par conséquent de causer un déni de service via un trafic non spécifié vers lôadresse IP dôadministration.			
jgaa -- warftpd	Une vulnérabilité non spécifiée dans War FTP Daemon (warftpd) 1.82, lorsquôil est en exécution comme un service Windows, permet à des attaquants distants de causer un déni de service (panne) et éventuellement dôexécuter un code arbitraire via des vecteurs inconnus liés aux messages de journalisation (log) et au « gestionnaire interne des logs dans Windows Event log »	31/03/2014	10.0	CVE-2013-2278
koushik_dutta -- superuser	Le paquet CyanogenMod/ClockWorkMod/Koush Superuser 1.0.2.1 pour Android permet à des attaquants dôobtenir des privilèges via des métacaractères du shell avec lôoption ï c vers /system/xbin/su.	31/03/2014	10.0	CVE-2013-6769
koushik_dutta -- superuser	Le paquet CyanogenMod/ClockWorkMod/Koush Superuser 1.0.2.1 pour Android 4.3 et 4.4 ne restreint pas correctement lôensemble des utilisateurs qui peuvent exécuter /system/xbin/su avec lôoption --daemon, ce qui permet à des attaquants dôobtenir des privilèges en prenant appui sur lôaccès à un shell ADB et un certain UID de Linux, et ainsi créer des scripts chevaux de Troyes.	31/03/2014	7.6	CVE-2013-6770
linux -- linux_kernel	Une situation de compétition dans la fonction ath_tx_aggr_sleep dans drivers/net/wireless/ath/ath9k/xmit.c dans le noyau Linux avant 3.13 permet à des attaquants distants de causer un déni de service (panne système) par l'intermédiaire d'une grande quantité de trafic de réseau qui déclenche certaines suppressions de liste.	01/04/2014	7.1	CVE-2014-2672
raoul_proenca -- gnew	De nombreuses vulnérabilités injection SQL dans Gnew 2013.1 permettent à des attaquants distants dôexécuter des commandes SQL arbitraires via les paramètres (1) answer_id ou (2) question_id vers polls/vote.php, (3) le paramètre story_id vers comments/add.php ou (4) comments/edit.php ou (5) le paramètre thread_id vers posts/add.php. REMARQUE : Ce problème était fractionné en raison de différences entre chercheurs et dates de divulgation. CVE-2013-7349 couvre déjà les vecteurs suivants : paramètre news_id vers news/send.php, paramètre user_email vers users/register.php et paramètre thread_id vers posts/edit.php.	31/03/2014	7.5	CVE-2013-5640

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source dôinformation & de correctif
raoul_proenca -- gnew	De nombreuses vulnérabilités injection SQL permettent à des attaquants distants dôexécuter des commandes SQL arbitraires via (1) le paramètre news_id parameter vers news/send.php, (2) le paramètre thread_id vers posts/edit.php, ou (3) le paramètre user_email vers users/password.php ou (4) users/register.php. REMARQUE : ces problèmes étaient fractionnés dans CVE-2013-5640 en raison de différences entre chercheurs et dates de divulgation.	31/03/2014	7.5	CVE-2013-7349
samsung -- kies	Un dépassement de tampon dans la méthode PrepareSync dans le ActiveX control SyncService.dll dans Samsung Kies avant 2.5.1.12123_2_7 permet à des attaquants distants dôexécuter un code arbitraire via une longueur chaine de caractère dans lôargument du mot de passe.	04/04/2014	10.0	CVE-2012-6429
schneider-electric -- concept	De nombreux dépassements de piles dans ModbusDrv.exe dans Schneider Electric Modbus Serial Driver 1.10 à 3.2 permettent à des attaquants distants dôexécuter un code arbitraire via une grande valeur de la taille du tampon dans Modbus Application Header.	01/04/2014	9.3	CVE-2013-0662
schneider-electric -- opc_factory_server_tlxcdlfofs	De nombreux dépassements de tampons dans le control ActiveX OPC Automation 2.0 Server Object de Schneider Electric OPC Factory Server (OFS) TLXCDSUOFS33 3.5 et antérieures, TLXCDSTOFS33 3.5 et antérieures, TLXCDLUOFS33 3.5 et antérieures, TLXCDLTOFS33 3.5 et antérieures, and TLXCDLFOFS33 3.5 et antérieures permettent à des attaquants distants de provoquer un déni de service via de longs arguments vers des fonctions non spécifiées.	04/04/2014	7.8	CVE-2014-0789
sonatype -- nexus	Une vulnérabilité non spécifiée dans Sonatype Nexus OSS et Pro 2.4.0 à 2.7.1 permet à des attaquants de créer des comptes utilisateur arbitraires via des vecteurs inconnus liés à « un chemin dôexécution non authentifié »	31/03/2014	7.5	CVE-2014-2034
symantec -- liveupdate_administrator	La fonctionnalité mot-de-passe oublié dans forcepasswd.do dans lôinterface graphique utilisateur dôadministration dans Symantec LiveUpdate Administrator (LUA) 2.x avant 2.3.2.110 permet à des attaquants distants de réinitialiser arbitrairement des mots de passe en fournissant lôadresse e-mail associé avec un compte dôutilisateur.	28/03/2014	7.5	CVE-2014-1644
symantec -- liveupdate_administrator	Une vulnérabilité injection SQL dans forcepasswd.do dans lôinterface graphique utilisateur dôadministration	28/03/2014	7.5	CVE-2014-1645

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source dôinformation & de correctif
	dans Symantec LiveUpdate Administrator (LUA) 2.x avant 2.3.2.110 permet à des attaquants distants dôexécuter des commandes SQL arbitraires via des vecteurs non spécifiés.			
theforeman -- foreman	De nombreuses vulnérabilités injection SQL dans Foreman avant 1.0.2 permettent à des attaquants distants dôexécuter arbitrairement des commandes SQL via des paramètres non spécifiés vers (1) app/models/hostext/search.rb ou (2) app/models/puppetclass.rb, liés au mécanisme de recherche.	04/04/2014	7.5	CVE-2012-5648
tracker-software -- pdf-xchange	Un dépassement de tas dans Tracker Software PDF-XChange avant 2.5.208 permet à des attaquants distants dôexécuter arbitrairement un code via un entête Define Huffman Table falsifié dans un flux de fichier image JPEG dans un fichier PDF.	02/04/2014	9.3	CVE-2013-0729
vtiger -- vtiger_crm	De nombreuses vulnérabilités injection SQL dans vTiger CRM 5.0.0 à 5.4.0 permettent à des attaquants distants dôexécuter des commandes SQL arbitraires via (1) le paramètre picklist_name dans la méthode get_picklists vers soap/customerportal.php, (2) le paramètre where dans la méthode get_tickets_list vers soap/customerportal.php, ou (3) le paramètre emailaddress dans la méthode SearchContactsByEmail vers soap/vtigerolservice.php ; ou à des utilisateurs authentifiés à distance dôexécuter arbitrairement des commandes SQL via le (4) paramètre emailaddress dans la méthode SearchContactsByEmail vers soap/thunderbirdplugin.php.	02/04/2014	7.5	CVE-2013-3213
zyxel -- p-660h-61	Lôinterface web de gestion sur les dispositifs Zyxel P660 permet à des attaquants distants de provoquer un déni de service (rédemarrage) via une inondation par des paquets TCP SYN.	01/04/2014	7.8	CVE-2013-3588

Back to top

Vulnérabilités majeures

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source dôinformation & de correctif
apache -- commons_fileupload	MultipartStream.java dans Apache Commons FileUpload avant 1.3.1, tel que utilisé dans Apache Tomcat, JBoss Web et dôautres produits permet à des attaquants distants de provoquer	01/04/2014	5.0	CVE-2014-0050

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source dôinformation & de correctif
	un déni de service (boucle infinie et consommation de CPU) via un faux entête Content-Type qui contourne les conditions prévues pour une sortie de boucle.			
apache -- couchdb	Apache CouchDB 1.5.0 et versions antérieures permet à des attaquants distants de provoquer un déni de service (consommation CPU et mémoire) via the paramètre de comptage vers /_uuids.	28/03/2014	5.0	CVE-2014-2668
apple -- safari	WebKit, tel quôutilisé dans Apple Safari avant 6.1.3 et 7.x avant 7.0.3, ne valide pas correctement les messages IPC de WebProcess, ce qui permet à des attaquants distants de contourner un mécanisme de protection sandbox et de lire arbitrairement des fichiers en sôappuyant sur lôaccès à WebProcess.	02/04/2014	5.0	CVE-2014-1297
apple -- safari	WebKit, tel quôutilisé dans Apple Safari avant 6.1.3 et 7.x avant 7.0.3 permet à des attaquants distants dôexécuter un code arbitraire ou de provoquer un déni de service (corruption mémoire et panne dôapplication) via un faux site web, une vulnérabilité différente des autres CVEs de WebKit listées dans APPLE-SA-2014-04-01-1.	02/04/2014	6.8	CVE-2014-1298
apple -- safari	WebKit, tel quôutilisé dans Apple Safari avant 6.1.3 et 7.x avant 7.0.3, permet à des attaquants distants dôexécuter un code arbitraire ou causer un déni de service (corruption mémoire et panne dôapplication) via un faux site web, une vulnérabilité différente de celles des autres CVE de WebKit listées dans APPLE-SA-2014-04-01-1.	02/04/2014	6.8	CVE-2014-1299
apple -- safari	WebKit, tel quôutilisé dans Apple Safari avant 6.1.3 et 7.x avant 7.0.3, permet à des attaquants distants dôexécuter un code arbitraire ou causer un déni de service (corruption mémoire et panne dôapplication) via un faux site web, une vulnérabilité différente de celles des autres CVEs de WebKit listées dans APPLE-SA-2014-04-01-1.	02/04/2014	6.8	CVE-2014-1301
apple -- safari	WebKit, tel quôutilisé dans Apple Safari avant 6.1.3 et 7.x avant 7.0.3, permet à des attaquants distants dôexécuter un code arbitraire ou causer un déni de service (corruption mémoire et panne dôapplication) via un faux site web, une vulnérabilité différente de celles des autres CVEs de WebKit listées dans APPLE-SA-2014-04-01-1.	02/04/2014	6.8	CVE-2014-1302
apple -- safari	WebKit, tel quôutilisé dans Apple Safari avant 6.1.3 et 7.x avant 7.0.3, permet à des attaquants distants dôexécuter un code arbitraire ou causer un déni de service (corruption mémoire et panne dôapplication) via un faux site web, une vulnérabilité différente de celles des autres CVEs de WebKit listées dans APPLE-SA-2014-04-01-1.	02/04/2014	6.8	CVE-2014-1304
apple -- safari	WebKit, tel quôutilisé dans Apple Safari avant 6.1.3 et 7.x avant 7.0.3, permet à des attaquants distants dôexécuter un code arbitraire ou causer un déni de service (corruption mémoire et panne dôapplication) via un faux site web, une vulnérabilité différente de celles des autres CVEs de WebKit listées dans APPLE-SA-2014-04-01-1.	02/04/2014	6.8	CVE-2014-1305

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source dôinformation & de correctif
apple -- safari	WebKit, tel quôutilisé dans Apple Safari avant 6.1.3 et 7.x avant 7.0.3, permet à des attaquants distants dôexécuter un code arbitraire ou causer un déni de service (corruption mémoire et panne dôapplication) via un faux site web, une vulnérabilité différente de celles des autres CVE de WebKit listées dans APPLE-SA-2014-04-01-1.	02/04/2014	6.8	CVE-2014-1307
apple -- safari	WebKit, tel quôutilisé dans Apple Safari avant 6.1.3 et 7.x avant 7.0.3, permet à des attaquants distants dôexécuter un code arbitraire ou causer un déni de service (corruption mémoire et panne dôapplication) via un faux site web, une vulnérabilité différente de celles des autres CVE de WebKit listées dans APPLE-SA-2014-04-01-1.	02/04/2014	6.8	CVE-2014-1308
apple -- safari	WebKit, tel quôutilisé dans Apple Safari avant 6.1.3 et 7.x avant 7.0.3, permet à des attaquants distants dôexécuter un code arbitraire ou causer un déni de service (corruption mémoire et panne dôapplication) via un faux site web, une vulnérabilité différente de celles des autres CVE de WebKit listées dans APPLE-SA-2014-04-01-1.	02/04/2014	6.8	CVE-2014-1309
apple -- safari	WebKit, tel quôutilisé dans Apple Safari avant 6.1.3 et 7.x avant 7.0.3, permet à des attaquants distants dôexécuter un code arbitraire ou causer un déni de service (corruption mémoire et panne dôapplication) via un faux site web, une vulnérabilité différente de celles des autres CVE de WebKit listées dans APPLE-SA-2014-04-01-1.	02/04/2014	6.8	CVE-2014-1310
apple -- safari	WebKit, tel quôutilisé dans Apple Safari avant 6.1.3 et 7.x avant 7.0.3, permet à des attaquants distants dôexécuter un code arbitraire ou causer un déni de service (corruption mémoire et panne dôapplication) via un faux site web, une vulnérabilité différente de celles des autres CVE de WebKit listées dans APPLE-SA-2014-04-01-1.	02/04/2014	6.8	CVE-2014-1311
apple -- safari	WebKit, tel quôutilisé dans Apple Safari avant 6.1.3 et 7.x avant 7.0.3, permet à des attaquants distants dôexécuter un code arbitraire ou causer un déni de service (corruption mémoire et panne dôapplication) via un faux site web, une vulnérabilité différente de celles des autres CVE de WebKit listées dans APPLE-SA-2014-04-01-1.	02/04/2014	6.8	CVE-2014-1312
apple -- safari	WebKit, tel quôutilisé dans Apple Safari avant 6.1.3 et 7.x avant 7.0.3, permet à des attaquants distants dôexécuter un code arbitraire ou causer un déni de service (corruption mémoire et panne dôapplication) via un faux site web, une vulnérabilité différente de celles des autres CVE de WebKit listées dans APPLE-SA-2014-04-01-1.	02/04/2014	6.8	CVE-2014-1313
b2evolution -- b2evolution	Une vulnérabilité injection SQL dans blogs/admin.php dans b2evolution avant 4.1.7 permet à des administrateurs authentifiés à distance dôexécuter des commandes SQL arbitraires via le paramètre show_statuses[]. REMARQUE : cela peut être exploité en utilisant CSRF pour permettre à des attaquants distants non authentifiés d'exécuter des commandes arbitraires SQL.	02/04/2014	6.5	CVE-2013-2945

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source dôinformation & de correctif
b2evolution -- b2evolution	Une vulnérabilité Cross-site request forgery (CSRF) dans blogs/admin.php dans b2evolution avant 4.1.7 permet à des attaquants distants de détourner lâauthentification des administrateurs pour des requêtes qui mènent à attaques par injections SQL via le paramètre show_statuses[], lié à CVE-2013-2945.	02/04/2014	6.8	CVE-2013-7352
cartpauj -- mingle-forum	De nombreuses vulnérabilités cross-site scripting (XSS) dans le plugin Forum de Mingle avant 1.0.34 pour WordPress permettent à des attaquants distants dôinjecter un script web ou HTML arbitraire via (1) le paramètre search_words dans une action de recherche vers wpf.class.php ou (2) le paramètre togroupusers dans une action add_user_togroup vers fs-admin/fs-admin.php.	28/03/2014	4.3	CVE-2013-0734
cisco -- emergency_responder	Une vulnérabilité Cross-site scripting (XSS) dans UserServlet dans Cisco Emergency Responder (ER) 8.6 et antérieures permet à des attaquants distants dôinjecter un script web ou HTML arbitraire via un paramètre non spécifié, alias Bug ID CSCun24384.	04/04/2014	4.3	CVE-2014-2114
cisco -- emergency_responder	De multiples vulnérabilités cross-site request forgery (CSRF) dans les pages CERUserServlet dans Cisco Emergency Responder (ER) 8.6 et antérieures permettent à des attaquants distants de détourner lâauthentification dôutilisateurs arbitraires, alias Bug ID CSCun24250.	04/04/2014	6.8	CVE-2014-2115
cisco -- emergency_responder	Cisco Emergency Responder (ER) 8.6 et antérieures permet à des attaquants distants dôinjecter des pages web et modifier un contenu dynamique via des paramètres non spécifiés, alias Bug ID CSCun37882.	04/04/2014	4.3	CVE-2014-2116
cisco -- emergency_responder	De nombreuses vulnérabilités redirection ouverte dans Cisco Emergency Responder (ER) 8.6 et antérieures permettent à des attaquants distants de rediriger les utilisateurs vers des sites web arbitraires et mener des attaques phishing via des paramètres non spécifiés, alias Bug ID CSCun37909.	04/04/2014	4.3	CVE-2014-2117
cisco -- unity_connection	Une vulnérabilité Cross-site scripting (XSS) dans Web Inbox dans Cisco Unity Connection 8.6(2a)SU3 et antérieures permet à des attaquants distants dôinjecter des scripts web ou HTML arbitraires via un paramètre non spécifié, alias Bug ID CSCui33028.	01/04/2014	4.3	CVE-2014-2125
cisco -- ios	Le pilote de paquet dans Cisco IOS permet à des attaquants distants de causer un déni de service (rechargement de système) via des séries de paquets (1) Virtual Switching Systems (VSS) ou 2) Bidirectional Forwarding Detection (BFD), alias Bug IDs CSCug41049 and CSCue61890.	28/03/2014	6.1	CVE-2014-2131
cisco -- web_security_virtual_appliance	Une vulnérabilité injection CRLF dans le cadre web dans Cisco Web Security Appliance (WSA) 7.7 et antérieures permet à des attaquants distants dôinjecter des entêtes HTTP arbitraires via une fausse URL, alias Bug ID CSCuj61002.	01/04/2014	4.3	CVE-2014-2137
cisco -- security_manager	Une vulnérabilité injection CRLF dans le cadre web dans Cisco Security Manager 4.2 et	01/04/2014	4.3	CVE-2014-2138

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source dôinformation & de correctif
	antérieures permet à des attaquants distants dôinjecter des entêtes HTTP arbitraires et mener des attaques de redirection via une fausse URL, alias Bug ID CSCun82349.			
cisco -- ios	Lôimplémentation de IKE dans Cisco IOS 15.4(1)T et antérieures dans IOS XE permet à des attaquants distants de causer un déni de service (arrêt de lâassociation de sécurité) via de faux paquets Main Mode, alias Bug ID CSCun31021.	04/04/2014	5.0	CVE-2014-2143
dotcms -- dotcms	De nombreuses vulnérabilités cross-site scripting (XSS) dans dotCMS avant 2.3.2 permettent à des attaquants distants dôinjecter un script web ou HTML arbitraire via (1) le paramètre _loginUserName vers application/login/login.html, (2) le paramètre c/portal_public/login, ou (3) le paramètre email vers forgotPassword.	02/04/2014	4.3	CVE-2013-3484
emc -- vplex_geosynchrony	EMC VPLEX GeoSynchrony 4.x et 5.x avant 5.3 nôinclut pas le drapeau HTTPOnly dans lôentête Set-Cookie pour un cookie non spécifié, ce qui rend plus facile pour des attaquants distants dôobtenir potentiellement des informations sensibles via un script dâaccès dans ce cookie.	01/04/2014	6.0	CVE-2014-0634
emc -- rsa_adaptive_authentication_on-premise	Une vulnérabilité Cross-site scripting (XSS) dans lâapplication de gestion des cas en arrière-plan dans RSA Adaptive Authentication (On-Premise) 6.x et 7.x avant 7.1 SP0 P2 permet à des utilisateurs authentifiés à distance dôinjecter un script web ou HTML arbitraire via des vecteurs non spécifiés.	04/04/2014	4.3	CVE-2014-0637
emc -- rsa_adaptive_authentication_on-premise	Une vulnérabilité Cross-site scripting (XSS) dans RSA Adaptive Authentication (On-Premise) 6.x et 7.x avant 7.1 SP0 P2 permet à des attaquants distants dôinjecter un script web ou HTML arbitraire via des vecteurs impliquant des éléments FRAME, liée à un problème "cross-frame scripting".	04/04/2014	4.3	CVE-2014-0638
ganglia -- ganglia-web	Une vulnérabilité Cross-site scripting (XSS) dans views_view.php dans Ganglia Web 3.5.7 permet à des attaquants distants dôinjecter un script web ou HTML arbitraire via le paramètre view_name.	02/04/2014	4.3	CVE-2013-1770
gnu -- a2ps	Le script fixps dans a2ps 4.14 nôutilise pas lôoption dSAFER lorsquôil exécute gs, ce qui permet à des attaquants en fonction du contexte dôeffacer des fichiers arbitraires ou dôexécuter des commandes arbitraires via un faux fichier PostScript.	03/04/2014	6.8	CVE-2014-0466
gpeasy -- gpeasy_cms	Une vulnérabilité Cross-site scripting (XSS) dans la fonction NewSectionPrompt dans include/tool/editing_page.php dans gpEasy CMS 3.5.2 et antérieures permet à des attaquants distants dôinjecter un script web ou HTML arbitraire via le paramètre section dans une action new_section vers index.php.	28/03/2014	4.3	CVE-2013-0807
ibm -- websphere_portal	Une vulnérabilité Cross-site scripting (XSS) dans lôinterface utilisateur de WCM (Web Content Manager) dans IBM WebSphere Portal 6.1.0.x à 6.1.0.6 CF27, 6.1.5.x à 6.1.5.3 CF27, 7.0.0.x à 7.0.0.2 CF27, et 8.0.0.x avant 8.0.0.1 CF11	01/04/2014	4.3	CVE-2014-0828

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source dôinformation & de correctif
	permet à des attaquants distants dôinjecter un script web ou HTML arbitraires via des vecteurs non spécifiés.			
igor_sysoev -- nginx	Un dépassement de tas dans lôimplémentation de SPDY dans nginx 1.3.15 avant 1.4.7 et 1.5.x avant 1.5.12 permet à des attaquants distants dôexécuter un code arbitraire via une fausse requête.	28/03/2014	5.1	CVE-2014-0133
jeff_kreitner -- hms-testimonials	De nombreuses vulnérabilités cross-site request forgery (CSRF) dans le plugin HMS Testimonials avant 2.0.11 pour WordPress permettent à des attaquants distants de détourner lôauthentification des administrateurs pour des requêtes qui (1) ajoutent de nouveaux témoignages via la page hms-testimonials-addnew, (2) ajoutent de nouveaux groupes via la page hms-testimonials-addnewgroup, (3) changent les configurations par défault via la page hms-testimonials-settings, (4) changent les configuration avancées via la page hms-testimonials-settings-advanced, (5) changent les configurations personnalisées via la page hms-testimonials-settings-fields ou (6) changent les modèles de configuration via la page hms-testimonials-templates-new vers wp-admin/admin.php.	02/04/2014	6.8	CVE-2013-4240
jgaa -- warftpd	Une vulnérabilité format de chaine de caractère dans War FTP Daemon (warftpd) 1.82 RC 12 permet à des utilisateurs authentifiés à distance de provoquer un déni de service (panne) via des spécificateurs de format de caractère dans une commande LIST.	31/03/2014	4.0	CVE-2009-5141
koushik_dutta -- superuser	Une vulnérabilité de chemin de recherche non fiable dans le paquet CyanogenMod/ClockWorkMod/Koush Superuser 1.0.2.1 pour Android 4.2.x et antérieures permet à des attaquants de déclencher le lancement dôun Cheval de Troyes app_process via une variable dôenvironnement falsifiée du processus /system/xbin/su.	31/03/2014	5.0	CVE-2013-6768
linux -- linux_kernel	Une vulnérabilité « double free » dans la fonction ioctx_alloc dans fs/aio.c dans le noyau Linux antérieur à 3.12.4 permet à des utilisateurs locaux de causer un déni de service (panne système) ou éventuellement avoir des impacts non déterminés via des vecteurs impliquant une condition dôerreur dans la fonction aio_setup_ring.	01/04/2014	4.6	CVE-2013-7348
linux -- linux_kernel	La fonction arch_dup_task_struct dans lôimplémentation de Transactional Memory (TM) dans arch/powerpc/kernel/process.c dans le noyau Linux avant 3.13.7 sur les plateformes powerpc nôinteragit pas correctement avec les appels clone et système fork, ce qui permet à des utilisateurs locaux de provoquer un déni de service (Vérification de programme et arrêt de système) via certaines instructions qui sont exécutées avec le processeur dans lôétat de Transactional.	01/04/2014	4.7	CVE-2014-2673
linux -- linux_kernel	La fonction rds_iw_laddr_check dans net/rds/iw.c dans le noyau Linux jusquôà 3.14 permet à des	01/04/2014	4.7	CVE-2014-2678

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source dôinformation & de correctif
	utilisateurs locaux de provoquer un déni de service (déréférencement de pointeur NULL et arrêt système) ou éventuellement avoir dâautre impact non spécifié via un appel system de liaison pour un socket RDS sur un système qui manque de transports RDS.			
microsoft -- windows_media_player	Microsoft Windows Media Player (WMP) 11.0.5721.5230 permet à des attaquants distants de provoquer un déni de service (corruption mémoire) ou éventuellement avoir un autre impact non spécifié via un fichier WAV falsifié.	31/03/2014	6.8	CVE-2014-2671
mozilla -- firefox	La fonction saltProfileName dans base/GeckoProfileDirectories.java dans Mozilla Firefox jusquâà 28.0.1 sur Android compte sur lâapproche non forte dâAndroid dâalimentation de la fonction Math.random, ce qui rend plus facile à des attaquants de contourner un mécanisme de protection de profil à répartition aléatoire via une application falsifiée.	29/03/2014	5.0	CVE-2014-1516
openstack -- keystone	Le jeton dâarrière-plan memcache dans OpenStack Identity (Keystone) 2013.1 à 2.013.1.4, 2013.2 à 2013.2.2, et icehouse avant icehouse-3, lorsquôil délivre un jeton de confiance avec impersonation activé, nôinclut pas ce jeton dans la liste dôindex des jetons de confiance, ce empêche le jeton dêtre invalidé par une révocation globale et permet de contourner les restrictions dâaccès prévues.	01/04/2014	5.0	CVE-2014-2237
oracle -- vm_virtualbox	VBox/GuestHost/OpenGL/util/net.c in Oracle VirtualBox 4.2.x à 4.2.20 et 4.3.x avant 4.3.8, lorsquôil utilise lâaccélération 3D permet aux utilisateurs locaux du système dêexploitation hôte dêexécuter un code arbitraire sur le server Chromium via un faux pointeur de réseau de Chromium dans un message (1) CR_MESSAGE_READBACK ou (2) CR_MESSAGE_WRITEBACK vers le service VBoxSharedCrOpenGL, ce qui déclenche un déréférencement arbitraire de pointeur et une corruption mémoire. REMARQUE : ce problème était fusionné avec CVE-2014-0982 parce quôil est du même type de vulnérabilité affectant le même ensemble de versions. Tous les utilisateurs de CVE devraient se référer à CVE-2014-0981 au lieu de CVE-2014-0982.	31/03/2014	4.4	CVE-2014-0981
oracle -- vm_virtualbox	De nombreuses erreurs dôindex de tableau dans des programmes qui sont automatiquement générés par VBox/HostServices/SharedOpenGL/crserverlib/server_dispatch.py dans Oracle VirtualBox 4.2.x à 4.2.20 et 4.3.x avant 4.3.8, lorsque lâaccélération 3D est utilisée, permettent aux utilisateurs locaux du système dêexploitation hôte dêexécuter un code arbitraire sur le serveur Chromium via certains messages de CR_MESSAGE_OPCODES avec un index falsifié, qui ne sont pas correctement manipulés par (1) CR_VERTEXATTRIB4NUBARB_OPCODE vers la fonction crServerDispatchVertexAttrib4NubARB, (2)	31/03/2014	6.9	CVE-2014-0983

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source dôinformation & de correctif
	CR_VERTEXATTRIB1DARB_OPCODE vers la fonction crServerDispatchVertexAttrib1dARB, (3) CR_VERTEXATTRIB1FARB_OPCODE vers la fonction crServerDispatchVertexAttrib1fARB, (4) CR_VERTEXATTRIB1SARB_OPCODE vers la fonction crServerDispatchVertexAttrib1sARB, (5) CR_VERTEXATTRIB2DARB_OPCODE vers la fonction crServerDispatchVertexAttrib2dARB, (6) CR_VERTEXATTRIB2FARB_OPCODE vers la fonction crServerDispatchVertexAttrib2fARB, (7) CR_VERTEXATTRIB2SARB_OPCODE vers la fonction crServerDispatchVertexAttrib2sARB, (8) CR_VERTEXATTRIB3DARB_OPCODE vers la fonction crServerDispatchVertexAttrib3dARB, (9) CR_VERTEXATTRIB3FARB_OPCODE vers la fonction crServerDispatchVertexAttrib3fARB, (10) CR_VERTEXATTRIB3SARB_OPCODE vers la fonction crServerDispatchVertexAttrib3sARB, (11) CR_VERTEXATTRIB4DARB_OPCODE vers la fonction crServerDispatchVertexAttrib4dARB, (12) CR_VERTEXATTRIB4FARB_OPCODE vers la fonction crServerDispatchVertexAttrib4fARB et (13) CR_VERTEXATTRIB4SARB_OPCODE vers la fonction crServerDispatchVertexAttrib4sARB.			
pearson -- esis_enterprise_ student_information_ system	Une vulnérabilité Cross-site scripting (XSS) dans aal/loginverification.aspx dans Pearson eSIS Enterprise Student Information System permet à des attaquants distants dôinjecter un script web ou HTML arbitraire via des vecteurs non spécifiés.	01/04/2014	4.3	CVE-2014-1942
posh_project -- posh	La fonctionnalité remember me dans portal/scr_authentif.php dans POSH (alias Posh portal or Portaneo) 3.0, 3.2.1, 3.3.0 et antérieures stocke le nom dôutilisateur et le condensé MD5 du mot de passe dans un message texte en clair dans un cookie, ce qui permet à des attaquants dôobtenir des informations sensibles en lisant le cookie.	01/04/2014	5.0	CVE-2014-2212
postfix_admin_project -- postfix_admin	Une vulnérabilité injection SQL dans la fonction gen_show_status dans functions.inc.php dans Postfix Admin (alias postfixadmin) avant 2.3.7, permet à des utilisateurs authentifiés à distance dôexécuter des commandes SQL arbitraires via un nouvel alias.	02/04/2014	6.5	CVE-2014-2655
postgresql -- postgresql	PostgreSQL avant 8.4.20, 9.0.x avant 9.0.16, 9.1.x avant 9.1.12, 9.2.x avant 9.2.7, et 9.3.x avant 9.3.3 nôapplique pas correctement une restriction ADMIN OPTION, ce qui permet à des membres authentifiés à distance dans ce rôle dôajouter ou supprimer des utilisateurs arbitraires dans ce rôle en appelant la commande SET ROLE avant la commande associée GRANT.	31/03/2014	4.0	CVE-2014-0060
postgresql -- postgresql	Les fonctions de validation pour les langages procédurales (PLs) dans PostgreSQL avant 8.4.20, 9.0.x avant 9.0.16, 9.1.x avant 9.1.12, 9.2.x avant 9.2.7, et 9.3.x avant 9.3.3 permettent à des utilisateurs authentifiés à distance dôobtenir des privilèges via une fonction qui (1) est définie dans un autre langage ou (2) qui nôest pas autorisée à être directement appelée par les utilisateurs pour raisons de permissions.	31/03/2014	6.5	CVE-2014-0061

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source dôinformation & de correctif
postgresql -- postgresql	Une situation de compétition dans les commandes (1) CREATE INDEX et (2) ALTER TABLE non spécifiée, dans PostgreSQL avant 8.4.20, 9.0.x avant 9.0.16, 9.1.x avant 9.1.12, 9.2.x avant 9.2.7 et 9.3.x avant 9.3.3 permet à des utilisateurs authentifiés à distance de créer un index non autorisé ou lire des portions de tables non autorisées en créant ou en supprimant une table avec le même nom durant la fenêtre de temps.	31/03/2014	4.9	CVE-2014-0062
postgresql -- postgresql	De nombreux dépassement de tampons dans PostgreSQL avant 8.4.20, 9.0.x avant 9.0.16, 9.1.x avant 9.1.12, 9.2.x avant 9.2.7 et 9.3.x avant 9.3.3 permettent à des utilisateurs authentifiés à distance de provoquer un déni de service (arrêt) ou éventuellement dôexécuter un code arbitraire via des vecteurs liés à une constante incorrecte MAXDATELEN et des valeurs de durée de temps impliquant (1) des intervalles, (2) des horodatages ou (3) des fuseaux horaires, une autre vulnérabilité que celle de CVE-2014-0065.	31/03/2014	6.5	CVE-2014-0063
postgresql -- postgresql	De nombreux dépassements dôentier dans la fonction path_in et autres non spécifiées dans PostgreSQL avant 8.4.20, 9.0.x avant 9.0.16, 9.1.x avant 9.1.12, 9.2.x avant 9.2.7 et 9.3.x avant 9.3.3 permettent à des utilisateurs authentifiés à distance dôavoir des impacts non spécifiés et des vecteurs dôattaque, ce qui déclenche un dépassement de tampon. REMARQUE : cette référence a été découpée en raison des versions différentes affectées. Utiliser CVE-2014-2669 pour le vecteur hstore.	31/03/2014	6.5	CVE-2014-0064
postgresql -- postgresql	De nombreux dépassements de buffer dans PostgreSQL avant 8.4.20, 9.0.x avant 9.0.16, 9.1.x avant 9.1.12, 9.2.x avant 9.2.7 et 9.3.x avant 9.3.3 permettent à des utilisateurs authentifiés à distance dôavoir des impacts et des vecteurs dôattaque non spécifiés, une vulnérabilité différente de CVE-2014-0063.	31/03/2014	6.5	CVE-2014-0065
postgresql -- postgresql	Lôextension chkpass dans PostgreSQL avant 8.4.20, 9.0.x avant 9.0.16, 9.1.x avant 9.1.12, 9.2.x avant 9.2.7 et 9.3.x avant 9.3.3 ne vérifie pas correctement la valeur de retour de la fonction-bibliothèque crypt, ce qui permet à des utilisateurs authentifiés à distance de provoquer un déni de service (déréférencement pointeur NULL et arrêt) via des vecteurs non spécifiés.	31/03/2014	4.0	CVE-2014-0066
postgresql -- postgresql	La commande "make check" pour les suites de test dans PostgreSQL 9.3.3 et antérieures nôinvoque pas correctement initdb pour spécifier les spécifications de lôauthentification pour un cluster de base de données à utiliser pour les tests, ce qui permet à des utilisateurs locaux dôobtenir des privilèges en sôappuyant sur des accès à ce cluster.	31/03/2014	4.6	CVE-2014-0067
postgresql -- postgresql	De nombreux dépassements dôentier dans contrib/hstore/hstore_io.c dans PostgreSQL 9.0.x avant 9.0.16, 9.1.x avant 9.1.12, 9.2.x avant 9.2.7 et 9.3.x avant 9.3.3 permettent à des utilisateurs	31/03/2014	6.5	CVE-2014-2669

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source dôinformation & de correctif
	authentifiés à distance dôavoir un impact non spécifié via des vecteurs liés aux fonctions (1) hstore_recv, (2) hstore_from_arrays et (3) hstore_from_array dans contrib/hstore/hstore_io.c; et la fonction (4) hstoreArrayToPairs dans contrib/hstore/hstore_op.c, ce qui déclenche un dépassement de tampon. REMARQUE : ce problème était découpé de CVE-2014-0064 parce quôil affecte un ensemble différent de versions.			
pyyaml -- libyaml	Un dépassement de tas dans la fonction yaml_parser_scan_uri_escapes dans LibYAML avant 0.1.6 permet à des attaquants selon le contexte dôexécuter un code arbitraire via une longue séquence de caractères pourcentage encodé dans un URI dans un fichier YAML.	28/03/2014	6.8	CVE-2014-2525
qemu -- qemu	Un dépassement de tampon dans hw/scsi-disk.c dans le sous-système SCSI dans QEMU avant 0.15.2, tel quôutilisé par Xen, pourrait permettre à des utilisateurs locaux des hôtes ayant une permission dôaccès au CDROM de provoquer un déni de service (arrêt client) via une commande SAI READ CAPACITY SCSI falsifiée. REMARQUE : ceci est uniquement une vulnérabilité quand root a modifié manuellement certaines permissions ou des listes de contrôle dôaccès (ACLs).	01/04/2014	4.0	CVE-2011-3346
redhat -- network_satellite	Une vulnérabilité injection CRLF dans spacewalk-java avant 2.1.148-1 et Red Hat Network (RHN) Satellite 5.6 permet à des attaquants distants dôinjecter arbitrairement des entêtes HTTP et conduire à des attaques de fractionnement de réponses HTTP et des attaques par cross-site scripting (XSS) via un paramètre return_url.	01/04/2014	4.3	CVE-2013-1869
redhat -- jboss_web_framework_kit	La fonction doFilter dans webapp/PushHandlerFilter.java dans JBoss RichFaces 4.3.4, 4.3.5 et 5.x permet à des attaquants distants de provoquer un déni de service (consommation mémoire et erreur dôinsuffisance de mémoire) via un grand nombre de requêtes de poussée dôambiance malformées.	31/03/2014	4.3	CVE-2014-0086
redhat -- jboss_enterprise_application_platform	Red Hat JBoss Enterprise Application Platform (JBEAP) 6.2.2, lorsque utilisant Java Security Manager (JSM), nôapplique pas correctement les permissions définies par le fichier de politique, ce qui amène les applications à se voir autorisées la permission java.security.AllPermission et permettre à des attaquants distants de contourner les restrictions dôaccès prévues.	03/04/2014	5.8	CVE-2014-0093
roberta_bramski -- uploader	De nombreuses vulnérabilités cross-site scripting (XSS) dans views/notify.php dans le plugin Uploader 1.0.4 pour WordPress permettent à des attaquants distants dôinjecter un script web ou HTML arbitraire via le paramètre (1) notify ou (2) blog.	04/04/2014	4.3	CVE-2013-2287
siemens -- ruggedcom_rugged_operating_system	Lôinterface web de gestion dans Siemens RuggedCom ROS avant 3.11, ROS 3.11 avant 3.11.5 pour RS950G, ROS 3.12 et ROS 4.0 pour RSG2488 permet à des attaquants distants de	01/04/2014	5.0	CVE-2014-2590

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source dôinformation & de correctif
	causer un déni de service (indisponibilité dôinterface) via des paquets http falsifiés.			
splunk -- splunk	Une vulnérabilité Cross-site scripting (XSS) dans Splunk Web dans Splunk avant 5.0.8 permet à des attaquants distants dôinjecter un script web ou HTML arbitraire via des vecteurs non spécifiés.	02/04/2014	4.3	CVE-2014-2578
wpsymposium -- wp_symposium	Une vulnérabilité Open redirect dans invite.php dans le plugin WP Symposium 13.04 pour WordPress permet à des attaquants distants de rediriger des utilisateurs vers des sites web arbitraires et mener à des attaques dôhameçonnage via une URL dans le paramètre u.	28/03/2014	5.8	CVE-2013-2694
wpsymposium -- wp_symposium	Une vulnérabilité Cross-site scripting (XSS) dans invite.php dans le plugin WP Symposium avant 13.04 pour WordPress permet à des attaquants distants dôinjecter un script web ou HTML via le paramètre u.	28/03/2014	4.3	CVE-2013-2695
xcloner -- xcloner	Une vulnérabilité Cross-site request forgery (CSRF) dans le plugin XCloner avant 3.1.1 pour WordPress permet à des attaquants distants de détourner lôauthentification des administrateurs pour des requêtes qui créent des backups de site web via une requête vers wp-admin/plugins.php.	03/04/2014	6.8	CVE-2014-2340
xen -- xen	De nombreux dépassements dôentier dans les sous-opérations (1) FLASK_GETBOOL, (2) FLASK_SETBOOL, (3) FLASK_USER et (4) FLASK_CONTEXT_TO_SID dans le flask hypercall dans Xen 4.3.x, 4.2.x, 4.1.x, 3.2.x et antérieures, quand XSM est activé, permet à des utilisateurs locaux de provoquer un déni de service (défaut du processeur) via des vecteurs non spécifiés, une vulnérabilité différente de CVE-2014-1892, CVE-2014-1893 et CVE-2014-1894.	01/04/2014	5.2	CVE-2014-1891
xen -- xen	Xen 3.3 à 4.1, quand XSM est active, permet à des utilisateurs locaux de provoquer un déni de service via des vecteurs liés à « une grande allocation mémoire », une vulnérabilité différente de CVE-2014-1891, CVE-2014-1893 et CVE-2014-1894.	01/04/2014	5.2	CVE-2014-1892
xen -- xen	De nombreux dépassements dôentier dans les sous-opérations (1) FLASK_GETBOOL et (2) FLASK_SETBOOL dans flask hypercall dans Xen 4.1.x, 3.3.x, 3.2.x et antérieures, lorsque XSM est activé, permettent à des utilisateurs locaux de causer un déni de service (défaut de processeur) via des vecteurs non spécifiés, une vulnérabilité différente de CVE-2014-1891, CVE-2014-1892 et CVE-2014-1894.	01/04/2014	5.2	CVE-2014-1893
xen -- xen	De nombreux dépassements dôentier dans des sous-opérations non spécifiées dans flask hypercall dans Xen 3.2.x et antérieures, lorsque XSM est activé, permettent à des utilisateurs locaux de causer un déni de service (défaut du processeur) via des vecteurs non spécifiés, une vulnérabilité autre que CVE-2014-1891, CVE-2014-1892 et CVE-2014-1893.	01/04/2014	5.2	CVE-2014-1894

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source dôinformation & de correctif
xen -- xen	Une erreur Off-by-one dans la fonction flask_security_avc_cachestats dans xsm/flask/flask_op.c in Xen 4.2.x et 4.3.x, lorsque tous les processeurs physiques sont en utilisation, permet à des utilisateurs locaux de causer un déni de service (arrêt dôhôte) ou dôobtenir des informations sensibles de la mémoire de lôhyperviseur en sôappuyant sur un hypercall FLASK_AVC_CACHESTAT, ce qui déclenche un surpassement de lecture de tampon.	01/04/2014	5.8	CVE-2014-1895
xen -- xen	Les fonctions (1) do_send et (2) do_recv dans io.c in libvchan dans Xen 4.2.x, 4.3.x et 4.4-RC series permettent à des hôtes locaux de causer un déni de service ou éventuellement de gagner des privilèges via des boucles dôindex xenstore falsifiées, ce qui déclenche une «lire ou écrire après la fin de la boucle ».	01/04/2014	4.9	CVE-2014-1896
xen -- xen	Les opérations de contrôle HVMOP_set_mem_access de HVM dans Xen 4.1.x pour 32-bit et 4.1.x à 4.4.x pour 64-bit permettent à des administrateurs locaux des hôtes de causer un déni de service (consommation CPU) en sôappuyant sur lôaccès à certains services de domaines pour les hôtes HVM et une grande entrée.	28/03/2014	4.9	CVE-2014-2599
zingiri -- forums	Une vulnérabilité traversée de répertoire dans la fonction zing_forum_output dans forum.php dans le plugin du forum Zingiri (alias Forums) avant 1.4.4 pour WordPress permet à des attaquants distants de lire arbitrairement des fichiers via des .. (point point) dans le paramètre url vers index.php.	04/04/2014	5.0	CVE-2012-4920
zohocorp -- manageengine_opstor	Properties.do dans ZOHO ManageEngine OpStor avant build 8500 ne vérifie pas correctement les niveaux de privilège, ce qui permet à des utilisateurs authentifiés à distance dôobtenir des accès dôadministrateur en utilisant le nom de paramètre en conjonction avec une valeur vrai avec le paramètre édition.	29/03/2014	6.5	CVE-2014-0344

Back to top

Vulnérabilités mineures

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- websphere_portal	Une vulnérabilité Cross-site scripting (XSS) dans lôimplémentation de Social Rendering lors de lôintégration de IBM Connections dans IBM WebSphere Portal 8.0.0.x à 8.0.0.1 CF11 permet à des utilisateurs authentifiés à distance dôinjecter un script web ou HTML arbitraire via des vecteurs non spécifiés.	01/04/2014	3.5	CVE-2014-0901
otrs -- otrs	Une vulnérabilité Cross-site scripting (XSS) dans Open Ticket Request System (OTRS) 3.1.x avant 3.1.21, 3.2.x avant 3.2.16 et 3.3.x avant 3.3.6 permet à des utilisateurs authentifiés à distance dôinjecter un script web ou HTML arbitraire via des vecteurs liés aux champs dynamiques.	02/04/2014	3.5	CVE-2014-2553

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
redhat -- jboss_operations_network	Red Hat JBoss Operations Network (JON) avant 2.4.2 nâapplique pas correctement les permissions "modify resource" pour les utilisateurs authentifiés à distance lorsque la mise à jour dûne configuration est en train dêtre supprimée à partir de lîhistorique des propriétés des connexions de groupe, ce qui empêche de telles activités dêtre enregistrées dans la file des audits.	01/04/2014	3.5	CVE-2011-4573
redhat -- jboss_operations_network	Red Hat JBoss Operations Network (JON) avant 3.0.1 utilise les permissions 0777 pour le repertoire root lorsquîil installe un client distant, ce qui permet à des utilisateurs locaux de lire ou modifier des sous-répertoires et des fichiers à lîintérieur du répertoire racine, comme démontré en obtenant des informations dîidentifications de JON.	01/04/2014	3.7	CVE-2012-0032
redhat -- conga	Luci dans Red Hat Conga stocke the nom dîutilisateur et le mot de passe de lîutilisateur dans une chaine de caractère encodée sur Base64 dans le cookie __ac session, ce qui permet à des attaquants dîobtenir des privilèges en sâappuyant sur ce cookie. REMARQUE : ce problème a été découpé en raison de différences entre les types de vulnérabilités. Utiliser CVE-2013-7347 pour lâapplication incorrecte de lâexpiration de lîutilisateur.	31/03/2014	3.7	CVE-2012-3359
redhat -- conga	Luci dans Red Hat Conga nâapplique pas correctement lâexpiration de la session de lîutilisateur, ce qui pourrait permettre à des attaquants dîobtenir un accès à la session en lisant le cookie __ac session. REMARQUE : ce problème a été découpé en raison de différences entre les types de vulnérabilités. Utiliser CVE-2012-3359 pour le problème de stockage du cookie de lîutilisateur encodé sur une Base64.	31/03/2014	3.7	CVE-2013-7347
zohocorp -- manageengine_opstor	Une vulnérabilité Cross-site scripting (XSS) dans Properties.do in ZOHO ManageEngine OpStor avant build 8500 permet à des utilisateurs authentifiés à distance dîinjecter un script web ou HTML arbitraire via le paramètre nom, une vulnérabilité différente de celle décrite par CVE-2014-0344.	29/03/2014	3.5	CVE-2014-2670

Back to top

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