Bulletin hebdomadaire des vulnérabilités n°BV14-03

Date de publication : 17/04/2014

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 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 Info & Correctif

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source Info & Correctif
adobe -- adobe_air	Un dépassement de tampon dans Adobe Flash Player avant 11.7.700.275 et 11.8.x à 13.0.x avant 13.0.0.182 sur Windows et OS X et avant 11.2.202.350 sur Linux, Adobe AIR avant 13.0.0.83 sur Android, Adobe AIR SDK avant 13.0.0.83, et Adobe AIR SDK & Compiler avant 13.0.0.83 permet à des attaquants dœexécuter un code arbitraire via des vecteurs non-spécifiés.	08/04/2014	9.3	CVE-2014-0507
advanced_forum_signatures_project -- advanced_forum_signatures	De multiples vulnérabilités injection SQL dans signature.php dans le plugin Advanced Forum Signatures (alias afsignatures) 2.0.4 pour MyBB permettent à des attaquants distants dœexécuter des commandes SQL arbitraires via le paramètre (1) afs_type, (2) afs_background, (3) afs_showonline, (4) afs_bar_left, (5) afs_bar_center, (6) afs_full_line1, (7) afs_full_line2, (8) afs_full_line3, (9) afs_full_line4, (10) afs_full_line5, or (11) afs_full_line6. REMARQUE: la source de cette information est inconnue ; les détails sont obtenus uniquement à partir des informations de tiers.	08/04/2014	7.5	CVE-2011-5277
advanced_forum_signatures_project -- advanced_forum_signatures	Une vulnérabilité injection SQL dans signature.php dans le plugin Advanced Forum Signatures (alias afsignatures) 2.0.4 pour MyBB permet à des attaquants distants dœexécuter des commandes SQL arbitraires via le paramètre afs_bar_right.	08/04/2014	7.5	CVE-2011-5278
cacti -- cacti	Une vulnérabilité injection SQL dans graph_xport.php dans Cacti 0.8.8b permet à des attaquants distants dœexécuter des commandes SQL arbitraires via des vecteurs non spécifiés.	10/04/2014	7.5	CVE-2014-2708
cisco -- adaptive_security_appliance_software	Cisco Adaptive Security Appliance (ASA) Software 8.2 avant 8.2(5.47), 8.4 avant 8.4(7.5), 8.7 avant 8.7(1.11), 9.0 avant 9.0(3.10), et 9.1 avant 9.1(3.4) permet à des utilisateurs authentifiés à distance dœobtenir des privilèges en sœappuyant sur lœaccès niveau-0 dœASDM, aussi connue sous lœappellation Bug ID CSCuj33496.	10/04/2014	8.5	CVE-2014-2126
cisco -- adaptive_security_appliance_software	Cisco Adaptive Security Appliance (ASA) Software 8.x avant 8.2(5.48), 8.3 avant 8.3(2.40), 8.4 avant 8.4(7.9), 8.6 avant 8.6(1.13), 9.0 avant 9.0(4.1), et 9.1 avant 9.1(4.3) ne traite pas correctement les informations de gestion de session lors de la validation de privilège pour des	10/04/2014	8.5	CVE-2014-2127

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source Info & Correctif
	connexions VPN SSL au portail, ce qui permet aux utilisateurs authentifiés à distance d'obtenir des privilèges en établissant une session VPN SSL sans client et en entrant des URL frauduleux, aussi connue sous lâappellation Bug ID CSCul70099.			
cisco -- adaptive_security_appliance_software	Le moteur dôinspection SIP dans Cisco Adaptive Security Appliance (ASA) Software 8.2 avant 8.2(5.48), 8.4 avant 8.4(6.5), 9.0 avant 9.0(3.1), et 9.1 avant 9.1(2.5) permet à des attaquants distants de provoquer un déni de service (consommation mémoire ou rechargement de lâappareil) via de faux paquets SIP, aussi connue sous lâappellation Bug ID CSCuh44052.	10/04/2014	7.1	CVE-2014-2129
clip-bucket -- clipbucket	De nombreuses vulnérabilités injection SQL dans la fonction update_counter dans includes/functions.php dans ClipBucket 2.6 permettent à des attaquants distants dôexécuter des commandes SQL arbitraires via le paramètre time vers (1) videos.php ou (2) channels.php. REMARQUE : certains des détails sont obtenus à partir dôinformation de tiers.	08/04/2014	7.5	CVE-2012-6643
erlang-solutions -- mongooseim	Erlang Solutions MongooseIM jusquâà 1.3.1 rev. 2 ne restreint pas correctement le traitement dôéléments XML compressés, ce qui permet à des attaquants distants de provoquer un déni de service (consommation ressource) via un flux XMPP falsifié, aussi connu sous lâappellation attaque "xmppbomb".	10/04/2014	7.8	CVE-2014-2829
google -- chrome	Une vulnérabilité Cross-site scripting (XSS) dans la fonction Runtime_SetPrototype dans runtime.cc dans Google V8, tel quôutilisé dans Google Chrome avant 34.0.1847.116, permet à des attaquants distants dôinjecter un script web ou HTML via des vecteurs non spécifiés, aussi connu sous lâappellation "Universal XSS (UXSS)."	09/04/2014	7.5	CVE-2014-1716
google -- chrome	Google V8, tel quôutilisé dans Google Chrome avant 34.0.1847.116, nôutilise pas correctement les conversions de type numériques (numeric casts) lors de la manipulation de tableaux typés, ce qui permet à des attaquants distants de provoquer un déni de service (accès hors limites du tableau) ou éventuellement dôavoir un impact non spécifié via un code JavaScript trafiqué.	09/04/2014	7.5	CVE-2014-1717

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source Info & Correctif
google -- chrome	Un débordement d'entier dans la fonction SoftwareFrameManager::SwapToNewFrame dans content/browser/renderer_host/software_frame_manager.cc dans le logiciel compositor dans Google Chrome avant 34.0.1847.116 permet à des attaquants distants de provoquer un déni de service ou éventuellement avoir un autre impact non spécifié via des vecteurs qui déclenchent une tentative de cartographie d'une grande quantité de rendu de mémoire.	09/04/2014	7.5	CVE-2014-1718
google -- chrome	Une vulnérabilité Use-after-free dans la fonction WebSharedWorkerStub::OnTerminateWorkerContext dans content/worker/websharedworker_stub.cc dans l'implémentation de Web Workers dans Google Chrome avant 34.0.1847.116 permet à des attaquants distants de provoquer un déni de service (corruption de la mémoire tas) ou éventuellement avoir un autre effet non spécifié via des vecteurs qui déclenchent une terminaison SharedWorker lors du chargement d'un script.	09/04/2014	7.5	CVE-2014-1719
google -- chrome	Une vulnérabilité Use-after-free dans la fonction HTMLBodyElement::insertedInto dans core/html/HTMLBodyElement.cpp dans Blink, tel qu'utilisé dans Google Chrome avant 34.0.1847.116, permet à des attaquants distants de provoquer un déni de service ou éventuellement avoir un autre effet non spécifié via des vecteurs impliquant les attributs.	09/04/2014	7.5	CVE-2014-1720
google -- chrome	Google V8, tel qu'utilisé dans Google Chrome avant 34.0.1847.116, n'implémente pas correctement « lazy deoptimization », ce qui permet à des attaquants distants de provoquer un déni de service (corruption mémoire) ou éventuellement avoir un autre effet non spécifié via un faux code JavaScript, comme il a été démontré par une manipulation incorrecte d'une allocation de tas d'un nombre hors de l'intervalle des petits entiers (appelé smi).	09/04/2014	7.5	CVE-2014-1721
google -- chrome	Une vulnérabilité Use-after-free dans la fonction RenderBlock::addChildIgnoringAnonymousColumnBlocks dans core/rendering/RenderBlock.cpp dans Blink, tel qu'utilisé dans Google Chrome avant 34.0.1847.116, permet à des attaquants distants de provoquer un déni de service ou éventuellement avoir un autre effet non spécifié	09/04/2014	7.5	CVE-2014-1722

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source Info & Correctif
	via des vecteurs impliquant lâajout dûun nî ud enfant.			
google -- chrome	La fonction UnescapeURLWithOffsetsImp dans net/base/escape.cc dans Google Chrome avant 34.0.1847.116 ne gère correctement les Identificateurs de ressource internationalisés (IRI) bidirectionnels, ce qui rend plus facile à des attaquants distants dûusurper les URLs via lûutilisation falsifiée de texte Unicode en écriture droite vers la gauche (RTL).	09/04/2014	7.5	CVE-2014-1723
google -- chrome	Une vulnérabilité Use-after-free dans Free(b)soft Laboratory Speech Dispatcher 0.7.1, tel quûutilisé dans Google Chrome avant 34.0.1847.116, permet à des attaquants distants de provoquer un déni de service (application plantée) ou éventuellement dâavoir un autre effet non spécifié via des requêtes *text-to-speech*.	09/04/2014	7.5	CVE-2014-1724
google -- chrome	Une vulnérabilité Use-after-free dans content/renderer/renderer_webcolorchooser_impl.h dans Google Chrome avant 34.0.1847.116 permet à des attaquants distants de provoquer un déni de service ou éventuellement avoir un autre effet non spécifié via des vecteurs liés aux formulaires.	09/04/2014	7.5	CVE-2014-1727
google -- chrome	De multiples vulnérabilités non spécifiées dans Google Chrome avant 34.0.1847.116 permettent à des attaquants de provoquer un déni de service ou éventuellement avoir un autre effet via des vecteurs inconnus.	09/04/2014	7.5	CVE-2014-1728
google -- chrome	De nombreuses vulnérabilités non spécifiées dans Google V8 avant 3.24.35.22, tel quûutilisé dans Google Chrome avant 34.0.1847.116, permettent à des attaquants de provoquer un déni de service ou éventuellement avoir un autre effet via des vecteurs non connus.	09/04/2014	7.5	CVE-2014-1729
igniterealtime -- openfire	Ignite Realtime Openfire avant 3.9.2 ne restreint pas correctement le traitement des éléments XML compressés, ce qui permet à des attaquants distants de provoquer un déni de service (consommation ressources) via un flux XMPP falsifié, aussi connu sous lâappellation dâattaque "xmppbomb".	10/04/2014	7.8	CVE-2014-2741
isode -- m-link	Isode M-Link avant 16.0v7 ne restreint pas correctement le traitement des éléments XML compressés, ce qui permet à des attaquants distants de provoquer un déni de service	10/04/2014	7.8	CVE-2014-2742

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source Info & Correctif
	(consommation de ressources) via un flux XMPP falsifié, aussi connu sous lâappellation dâattaque "xmppbomb".			
lightwitch -- metronome	plugins/mod_compression.lua dans Lightwitch Metronome jusquâà 3.4 ne restreint pas correctement le traitement des éléments XML compressés, ce qui permet à des attaquants distants de provoquer un déni de service (consommation ressources) via un flux XMPP falsifié, aussi connu sous lâappellation dâattaque "xmppbomb".	10/04/2014	7.8	CVE-2014-2743
lightwitch -- metronome	plugins/mod_compression.lua dans (1) Prosody avant 0.9.4 et (2) Lightwitch Metronome jusquâà 3.4 négocie une compression de flux alors quâune session est non authentifiée, ce qui permet à des attaquants distants de provoquer un déni de service (consommation ressources) via des éléments XML compressées dans un flux XMPP, aussi connu sous lâappellation dâattaque "xmppbomb".	10/04/2014	7.8	CVE-2014-2744
microsoft -- internet_explorer	Microsoft Internet Explorer 9 permet à des attaquants distants dâexécuter un code arbitraire ou provoquer un déni de service (corruption mémoire) via un site web trafiqué, aussi connu sous « Vulnérabilité de la corruption mémoire dâInternet Explorer », une vulnérabilité différente de CVE-2014-1751 et CVE-2014-1755.	08/04/2014	9.3	CVE-2014-0235
microsoft -- internet_explorer	Microsoft Internet Explorer 9 permet à des attaquants distants dâexécuter un code arbitraire ou provoquer un déni de service (corruption mémoire) via un site web trafiqué, aussi connu sous le nom de « Vulnérabilité de la corruption mémoire dâInternet Explorer », une vulnérabilité différente de CVE-2014-0235 et CVE-2014-1755.	08/04/2014	9.3	CVE-2014-1751
microsoft -- internet_explorer	Microsoft Internet Explorer 6 et 7 permet à des attaquants distants dâexécuter un code arbitraire ou provoquer un déni de service (corruption mémoire) via un site web trafiqué, aussi connu sous le nom de « Vulnérabilité de la corruption mémoire dâInternet Explorer ».	08/04/2014	9.3	CVE-2014-1752
microsoft -- internet_explorer	Microsoft Internet Explorer 6 à 9 permet à des attaquants distants dâexécuter un code arbitraire ou provoquer un déni de service (corruption mémoire) via un site web trafiqué, aussi connu sous le nom de « Vulnérabilité de la corruption mémoire dâInternet Explorer ».	08/04/2014	9.3	CVE-2014-1753

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source Info & Correctif
microsoft -- internet_explorer	Microsoft Internet Explorer 9 permet à des attaquants distants dê exécuter un code arbitraire ou provoquer un déni de service (corruption mémoire) via un site web trafiqué, aussi connu sous le nom de « Vulnérabilité de la corruption mémoire dî Internet Explorer ».	08/04/2014	9.3	CVE-2014-1755
microsoft -- office_compatibility_pack	Microsoft Word 2007 SP3 et 2010 SP1 et SP2, et Office Compatibility Pack SP3, allouent la mémoire de façon incorrecte pour les conversions de fichier du format binaire (.doc) vers un format plus récent, ce qui permet à des attaquants distants dê exécuter un code arbitraire via un document trafiqué, aussi connue sous le nom de « Vulnérabilité du convertisseur de format de fichier de Microsoft Office »	08/04/2014	9.3	CVE-2014-1757
microsoft -- word	Un débordement de pile dans Microsoft Word 2003 SP3 permet à des attaquants distants dê exécuter un code arbitraire via un document trafiqué, aussi connue sous le nom de « Vulnérabilité de débordement de pile de Microsoft Office »	08/04/2014	9.3	CVE-2014-1758
microsoft -- publisher	pubconv.dll dans Microsoft Publisher 2003 SP3 et 2007 SP3 permet à des attaquants distants dê exécuter un code arbitraire ou provoquer un déni de service (déréférencement incorrect de pointeur et crash dê application) via un fichier .pub trafiqué, aussi connue sous le nom de ñ Vulnérabilité de déréférencement arbitraire de pointeur ò	08/04/2014	9.3	CVE-2014-1759
microsoft -- internet_explorer	Microsoft Internet Explorer 11 permet à des attaquants distants dê exécuter un code arbitraire ou provoquer un déni de service (corruption mémoire) via un site web trafiqué, aussi connu sous le nom de « Vulnérabilité de corruption mémoire dî Internet Explorer »	08/04/2014	9.3	CVE-2014-1760
pearson -- esis_enterprise_student_information_system	Une vulnérabilité injection SQL dans la fonctionnalité de réinitialisation de mot de passe dans Pearson eSIS Enterprise Student Information System, peut-être 3.3.0.13 et précédentes, permet à des attaquants distants dê exécuter des commandes SQL arbitraires via le nouveau mot de passe.	10/04/2014	7.5	CVE-2014-1455
prosody -- prosody	Prosody avant 0.9.4 ne restreint pas correctement le traitement des éléments XML compressés, ce qui permet à	10/04/2014	7.8	CVE-2014-2745

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source Info & Correctif
	des attaquants distants de provoquer un déni de service (consommation ressource) via un flux XMPP trafiqué, aussi connu sous le nom dôattaque "xmppbomb", lié à core/portmanager.lua et util/xmppstream.lua.			
sap -- bi_universal_data_integration	Une vulnérabilité injection SQL dans SAP BI Universal Data Integration permet à des attaquants distants dôexécuter des commandes SQL arbitraires via des vecteurs non spécifiés, lié au schéma J2EE.	10/04/2014	7.5	CVE-2013-7355
sap -- adminadapter	Une vulnérabilité non spécifiée dans SAP adminadapter permet à des attaquants distants de lire ou écrire des fichiers arbitraires via des vecteurs inconnus.	10/04/2014	7.5	CVE-2013-7360
sap -- ccms_agent	Une fonction RFC non spécifiée dans SAP CCMS Agent permet à des attaquants distants dôexécuter des commandes arbitraires via des vecteurs inconnus.	10/04/2014	7.5	CVE-2013-7362
sap -- solution_manager	Une vulnérabilité non spécifiée dans lôagent Diagnostics (SMD) dans SAP Solution Manager permet à des attaquants distants dôobtenir des informations sensibles, modifier la configuration des applications, et installer ou désinstaller des applications via des vecteurs impliquant le protocole P4.	10/04/2014	7.5	CVE-2013-7363
sap -- netweaver	Un service central J2EE dans le moteur J2EE dans SAP NetWeaver ne restreint pas correctement lôaccès, ce qui permet à des attaquants distants de lire ou écrire sur des fichiers arbitraires via des vecteurs non connus.	10/04/2014	7.5	CVE-2013-7364
sap -- enterprise_portal	SAP Enterprise Portal ne restreint pas correctement lôaccès aux pages de configuration de Federation, ce qui permet à des attaquants distants dôobtenir des privilèges via des vecteurs non spécifiés.	10/04/2014	7.5	CVE-2013-7367
sap -- enhancement_package	Lôinstallation de Security Audit Log dans SAP Enhancement Package (EHP) 6 pour SAP ERP 6.0 permet à des attaquants distants de modifier ou supprimer arbitrairement des classes de log via des vecteurs non spécifiés. REMARQUE : certains des détails de lôinformation sont obtenus via des tiers.	10/04/2014	7.5	CVE-2014-2748
sap -- print_and_output_management	SAP Print et Output Management ont des paramètres dôauthentification codés en dur, ce qui rend plus facile à des attaquants distants dôobtenir des accès via des vecteurs	10/04/2014	7.5	CVE-2014-2751

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source Info & Correctif
	non spécifiés.			
sap -- business_object_processing_framework_for_abap	SAP Business Object Processing Framework (BOPF) pour ABAP a des paramètres dâauthentification codes en dur, ce qui rend plus facile pour des attaquants distants dôobtenir des accès via des vecteurs non spécifiés.	10/04/2014	7.5	CVE-2014-2752
tibco -- rendezvous	Un débordement de tampon dans Rendezvous Daemon (rvd), Rendezvous Routing Daemon (rvrd), Rendezvous Secure Daemon (rvsd), et Rendezvous Secure Routing Daemon (rvsrd) dans TIBCO Rendezvous avant 8.4.2, Messaging Appliance avant 8.7.1, et Substation ES avant 2.8.1 permet à des attaquants distants dôexécuter un code arbitraire en sâappuyant sur lâaccès à un client connecté directement et en transmettant de fausses données.	08/04/2014	7.5	CVE-2014-2543
tibco -- analyst	Une vulnérabilité non spécifiée dans Spotfire Web Player Engine, Spotfire Desktop, et Spotfire Server Authentication Module dans TIBCO Spotfire Server 3.3.x avant 3.3.4, 4.5.x avant 4.5.1, 5.0.x avant 5.0.2, 5.5.x avant 5.5.1, et 6.x avant 6.0.2; Spotfire Professional 4.0.x avant 4.0.4, 4.5.x avant 4.5.2, 5.0.x avant 5.0.2, 5.5.x avant 5.5.1, et 6.x avant 6.0.1; Spotfire Web Player 4.0.x avant 4.0.4, 4.5.x avant 4.5.2, 5.0.x avant 5.0.2, 5.5.x avant 5.5.1, et 6.x avant 6.0.1; Spotfire Automation Services 4.0.x avant 4.0.4, 4.5.x avant 4.5.2, 5.0.x avant 5.0.2, 5.5.x avant 5.5.1, et 6.x avant 6.0.1; Spotfire Deployment Kit 4.0.x avant 4.0.4, 4.5.x avant 4.5.2, 5.0.x avant 5.0.2, 5.5.x avant 5.5.1, and 6.x avant 6.0.1; Spotfire Desktop 6.x avant 6.0.1; et Spotfire Analyst 6.x avant 6.0.1 permet à des attaquants distants dôexécuter un code arbitraire via des vecteurs inconnus.	09/04/2014	7.5	CVE-2014-2544
tigase -- tigase	net/IOService.java dans Tigase avant 5.2.1 ne restreint pas correctement le traitement dõéléments XML compressés, ce qui permet à des attaquants distants de provoquer un déni de service (consommation ressources) via un flux XMPP trafiqué, aussi connue sous le nom dâattaque "xmppbomb".	10/04/2014	7.8	CVE-2014-2746

Retour haut de page

Vulnérabilités majeures

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source Info & Correctif
adobe -- adobe_air	Adobe Flash Player avant 11.7.700.275 et 11.8.x à 13.0.x avant 13.0.0.182 sur Windows et OS X et avant 11.2.202.350 sur Linux, Adobe AIR avant 13.0.0.83 sur Android, Adobe AIR SDK avant 13.0.0.83, et Adobe AIR SDK & Compiler avant 13.0.0.83 permettent à des attaquants distants de contourner des restrictions d'accès prévues et d'obtenir des informations sensibles via des vecteurs non spécifiés.	08/04/2014	5.0	CVE-2014-0508
adobe -- adobe_air	Une vulnérabilité Cross-site scripting (XSS) dans Adobe Flash Player avant 11.7.700.275 et 11.8.x à 13.0.x avant 13.0.0.182 sur Windows et OS X et avant 11.2.202.350 sur Linux, Adobe AIR avant 13.0.0.83 sur Android, Adobe AIR SDK avant 13.0.0.83, et Adobe AIR SDK & Compiler avant 13.0.0.83 permet à des attaquants distants d'injecter un script web ou HTML arbitraire via des vecteurs non spécifiés.	08/04/2014	4.3	CVE-2014-0509
cisco -- adaptive_security_appliance_software	L'implémentation de VPN SSL dans Cisco Adaptive Security Appliance (ASA) Software 8.2 avant 8.2(5.47, 8.3 avant 8.3(2.40), 8.4 avant 8.4(7.3), 8.6 avant 8.6(1.13), 9.0 avant 9.0(3.8), et 9.1 avant 9.1(3.2) permet à des attaquants distants de contourner l'authentification via (1) une valeur de cookie trafiquée à l'intérieur des données HTTP POST ou (2) une URL trafiquée, aussi connue le nom de Bug ID CSCua85555.	10/04/2014	5.0	CVE-2014-2128
cisco -- ons_15454	La fonctionnalité de fin-de-session dans les cartes-contrôleurs de Cisco ONS 15454 avec le logiciel 9.6 et antérieurs n'initialise pas un pointeur non spécifié, ce qui permet à des utilisateurs authentifiés à distance de causer un déni de service (réinitialisation de la carte) via des actions frauduleuses de fermeture de sessions, aussi connue sous le nom de Bug ID CSCug97416.	10/04/2014	4.0	CVE-2014-2141
cisco -- ios_xr	Cisco IOS XR n'entrave correctement pas les paquets ICMPv6 de redirection, ce qui permet à des attaquants distants de provoquer un déni de service (rupture de transit de IPv4 et IPv6) via de	05/04/2014	6.1	CVE-2014-2144

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source Info & Correctif
	messages de redirection trafiqués, aussi connu sous le nom de Bug ID CSCum14266.			
cisco -- unity_connection	Une vulnérabilité de traversée de répertoire dans les API de messagerie dans Cisco Unity Connection permet à des utilisateurs authentifiés à distance de lire des fichiers arbitraires via des vecteurs liés à des contraintes d'accès non appliquées pour des fichiers .wav et le type MIME audio/x-wav, aussi connu sous le nom de Bug ID CSCun91071.	05/04/2014	4.0	CVE-2014-2145
clip-bucket -- clipbucket	Une vulnérabilité Cross-site scripting (XSS) dans ClipBucket 2.6 permet à des attaquants distants d'injecter un script web ou HTML arbitraire via le paramètre type vers view_channel.php. REMARQUE : la source de cette information est indéterminée, les détails sont obtenus uniquement à partir d'information d'un tiers.	08/04/2014	4.3	CVE-2012-6642
clip-bucket -- clipbucket	De nombreuses vulnérabilités cross-site scripting (XSS) dans ClipBucket 2.6 permettent à des attaquants distants d'injecter un script web ou HTML arbitraire via (1) le paramètre cat vers channels.php, (2) collections.php, (3) groups.php, ou (4) videos.php; (5) le paramètre query vers search_result.php; ou (6) le paramètre type vers view_collection.php ou (7) view_item.php.	08/04/2014	4.3	CVE-2012-6644
cms_tree_page_view_project -- cms_tree_page_view	Une vulnérabilité Cross-site scripting (XSS) dans la fonction cms_tpv_admin_head dans functions.php dans le plugin CMS Tree Page View avant 0.8.9 pour WordPress permet à des attaquants distants d'injecter un script web ou HTML arbitraire via le paramètre cms_tpv_view vers wp-admin/options-general.php.	07/04/2014	4.3	CVE-2012-1834
danielb -- finder	Une vulnérabilité Cross-site scripting (XSS) dans le module Finder avant 6.x-1.26, 7.x-1.x, et 7.x-2.x avant 7.x-2.0-alpha8 pour Drupal permet à des attaquants distants d'injecter un script web ou HTML arbitraire via des vecteurs non spécifiés liés aux « fonctionnalités des boutons checkbox et	08/04/2014	4.3	CVE-2012-1561

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source Info & Correctif
	radio »			
danielb -- finder	Une vulnérabilité Cross-site scripting (XSS) dans la fonctionnalité autocomplete dans le module Finder 6.x-1.x avant 6.x-1.26, 7.x-1.x, et 7.x-2.x avant 7.x-2.0-alpha8 pour Drupal permet à des attaquants distants dôinjecter un script web ou HTML arbitraire via le titre dôun nî ud, une vulnérabilité différente de CVE-2012-1561.	08/04/2014	4.3	CVE-2012-6645
david_paleino -- wicd	La fonction SetWiredProperty dans lôinterface D-Bus dans WICD avant 1.7.2 permet à des utilisateurs locaux dôécrire arbitrairement des paramètres de configuration et obtenir des privilèges via un nom de propriété falsifié dans un message dbus.	07/04/2014	6.9	CVE-2012-2095
dell -- openmanage_server_administrator	Une vulnérabilité « Open redirect » dans Dell OpenManage Server Administrator (OMSA) avant 7.3.0 permet à des attaquants distants de rediriger des utilisateurs vers des sites web arbitraires et conduire à attaques par hameçonnage via des URLs dans le fichier de paramétrage dans HelpViewer.	10/04/2014	5.8	CVE-2013-0740
dvs_custom_notification_project -- dvs_custom_notification	De nombreuses vulnérabilités cross-site request forgery (CSRF) dans le plugin DVS Custom Notification 1.0.1 et précédentes pour WordPress permettent à des attaquants distants de détourner lôauthentification des administrateurs pour des requêtes qui (1) changent les paramètres des applications ou (2) qui mènent à des attaques cross-site scripting (XSS).	10/04/2014	6.8	CVE-2012-4921
fortinet -- fortiadc-1000e	Une vulnérabilité Cross-site scripting (XSS) dans lôinterface web dôadministration dans FortiADC avec le micrologiciel avant 3.2.1 permet à des attaquants dôinjecter un script web ou HTML arbitraire via le paramètre locale vers gui_partA/.	10/04/2014	4.3	CVE-2014-0331
google -- chrome	La fonction base64DecodeInternal dans wtf/text/Base64.cpp dans Blink, tel quôutilisé dans Google Chrome avant 34.0.1847.116, ne gère pas correctement les données chaine de caractères	09/04/2014	5.0	CVE-2014-1725

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source Info & Correctif
	composées exclusivement de caractères espace, ce qui permet à des attaquants distants de provoquer un déni de service (lecture hors des limites) via un appel à la méthode window.atob.			
google -- chrome	L'implémentation de drag dans Google Chrome avant 34.0.1847.116 permet à des utilisateurs assistés à distance mués en attaquants de contourner le « Same Origin Policy » et falsifier des noms de chemin d'accès locaux en tirant parti de l'accès au rendu.	09/04/2014	4.3	CVE-2014-1726
horde -- groupware	Une vulnérabilité Cross-site scripting (XSS) dans js/compose-dimp.js dans Horde Internet Mail Program (IMP) avant 5.0.24, tel qu'utilisé dans Horde Groupware Webmail Edition avant 4.0.9, permet à des attaquants distants d'injecter un script web ou HTML arbitraire via un nom trafiqué pour un fichier attaché, lié à la vue dynamique.	05/04/2014	4.3	CVE-2012-5565
horde -- groupware	De nombreuses vulnérabilités cross-site scripting (XSS) dans Horde Kronolith Calendar Application H4 avant 3.0.17, tel qu'utilisé dans Horde Groupware Webmail Edition avant 4.0.8, permettent à des attaquants distants d'injecter un script web ou HTML arbitraire via la (1) vue task ou (2) la vue search.	05/04/2014	4.3	CVE-2012-5566
horde -- groupware	De nombreuses vulnérabilités cross-site scripting (XSS) dans Horde Kronolith Calendar Application H4 avant 3.0.18, tel qu'utilisé dans Horde Groupware Webmail Edition avant 4.0.9, permettent à des attaquants distants d'injecter un script web ou HTML arbitraire via des paramètres falsifiés de localisation des événements dans les champs (1) month, (2) monthlist ou (3) prevmonthlist, en relation avec les blocs du portail.	05/04/2014	4.3	CVE-2012-5567
horde -- groupware	Une vulnérabilité Cross-site scripting (XSS) dans Horde Internet Mail Program (IMP) avant 5.0.22, tel qu'utilisé dans Horde Groupware Webmail Edition avant 4.0.9, permet à des attaquants distants d'injecter un script web ou HTML arbitraire via une	05/04/2014	4.3	CVE-2012-6640

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source Info & Correctif
	image SVG trafiquée en fichier attaché, une vulnérabilité différente de CVE-2012-5565.			
hp -- icewall_identity_manager	Une vulnérabilité non spécifiée dans HP IceWall Identity Manager 4.0 à SP1 et 5.0 et IceWall SSO 10.0 Password Reset Option, lorsque Apache Commons FileUpload est utilisé permet à des utilisateurs authentifiés à distance de provoquer un déni de service via des vecteurs inconnus.	05/04/2014	4.0	CVE-2014-2600
huawei -- echo_life	Une vulnérabilité Cross-site scripting (XSS) dans l'interface web sur les routeurs Huawei Echo Life HG8247 munis du logiciel avant V100R006C00SPC127 permet à des attaquants distants d'injecter un script web ou HTML arbitraire via une tentative de connexion TELNET invalide avec un faux nom d'utilisateur qui n'est pas correctement géré lors de la construction de la vue du log des « tentatives échouées de connexion par telnet ».	05/04/2014	4.3	CVE-2014-0337
ibm -- optim_workload_replay	Une vulnérabilité Cross-site scripting (XSS) dans IBM InfoSphere Optim Workload Replay 1.1 permet à des attaquants distants d'injecter un script web ou HTML arbitraire via une URL trafiquée.	05/04/2014	4.3	CVE-2014-0827
ibm -- business_process_manager	L'implémentation de User Attribute dans IBM Business Process Manager (BPM) 7.5.x à 7.5.1.2, 8.0.x à 8.0.1.2, et 8.5.x à 8.5.0.1 ne vérifie pas l'autorisation de l'accès en lecture ou écriture des valeurs des attributs, ce qui permet à des utilisateurs authentifiés à distance d'obtenir des informations sensibles, configure des emails de notification ou modifier des assignations de tâches via des appels REST API.	10/04/2014	6.0	CVE-2014-0908
ibm -- spss_analytic_server	IBM SPSS Analytic Server 1.0 avant IF002 et 1.0.1 avant IF004 enregistre les mots de passe en clair, ce qui permet aux utilisateurs distants à distance d'obtenir des informations sensibles via des vecteurs non précisés.	10/04/2014	4.0	CVE-2014-0920

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source Info & Correctif
jeremy_massel -- underconstruction	Une vulnérabilité Cross-site request forgery (CSRF) dans le plugin underConstruction avant 1.09 pour WordPress permet à des attaquants distants de détourner lâauthentification des administrateurs pour des requêtes qui désactivent un plugin via des vecteurs non spécifiés.	10/04/2014	6.8	CVE-2013-2699
kernel -- linux-pam	De nombreuses vulnérabilités traversées de répertoire dans pam_timestamp.c dans le module pam_timestamp pour Linux-PAM (aka pam) 1.1.8 permettent à des utilisateurs locaux de créer des fichiers arbitraires ou éventuellement contourner lâauthentification via des .. (point point) dans la valeur (1) PAM_RUSER vers la function get_ruser ou la valeur (2) PAM_TTY vers la fonction check_tty, qui est utilisée par la fonction format_timestamp_name.	10/04/2014	5.8	CVE-2014-2583
lee_howard -- hylafax+	Un débordement de tas dans hfaxd dans HylaFAX+ 5.2.4 à 5.5.3, lorsque lâauthentification LDAP est utilisée, pourrait permettre à des attaquants distants de provoquer un déni de service (processus enfant planté) ou exécuter un code arbitraire via une longue commande USER.	06/04/2014	6.8	CVE-2013-5680
lesterchan -- wp-postviews	Une vulnérabilité Cross-site request forgery (CSRF) dans les options de la page dâadministration dans le plugin WP-PostViews avant 1.63 pourWordPress permet à des attaquants distants de détourner lâauthentification des administrateurs pour des requêtes qui changent les configurations du plugin via des vecteurs non précisés.	10/04/2014	6.8	CVE-2013-3252
microsoft -- windows_7	Une vulnérabilité de chemin de recherche non fiable dans Microsoft Windows XP SP2 et SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 et R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold et R2, et Windows RT Gold et 8.1 permet à des utilisateurs locaux dâobtenir des privilèges via un fichier cheval de Troyes cmd.exe dans le chemin de travail courant, tel que démontré	08/04/2014	6.9	CVE-2014-0315

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source Info & Correctif
	par un chemin qui contient un fichier avec une extension .cmd ou .bat, aussi connu sous lâappellation « Vulnérabilité de manipulation de fichier de Windows ».			
microsoft -- office	Lâanalyser XML dans Microsoft Office 2007 SP3, 2010 SP1 et SP2, et 2013, et Office pour Mac 2011, ne détecte pas correctement la récursivité pendant lâexpansion de lâentité, ce qui permet à des attaquants distants de provoquer un déni de service (consommation mémoire et persistance du plantage dâapplication) via un document XML trafiqué contenant un grand nombre de références à des entités imbriquées, comme démontré par un message email en texte/brut trafiqué vers Outlook, un problème similaire à CVE-2003-1564.	05/04/2014	5.0	CVE-2014-2730
openssl -- openssl	Lâimplémentation de (1) TLS et (2) DTLS dans OpenSSL 1.0.1 avant 1.0.1g ne gère pas correctement les paquets Heartbeat Extension, ce qui permet à des attaquants distants dâobtenir des informations sensibles de la mémoire dâun processus via des paquets trafiqués qui déclenchent un débordement de la lecture du tampon, tel que démontré par la lecture des clés privées, en relation avec d1_both.c and t1_lib.c, aussi connue sous lâappellation de bug Heartbleed (cî ur qui saigne)	07/04/2014	5.0	CVE-2014-0160
prestashop -- prestashop	Une vulnérabilité Cross-site scripting (XSS) dans redirect.php dans le module Socolissimo (modules/socolissimo/) dans PrestaShop avant 1.4.7.2 permet à des attaquants distants dâinjecter un script web ou HTML arbitraire via des vecteurs liés aux « noms et valeurs du paramètre ».	07/04/2014	4.3	CVE-2012-6641
prosody -- prosody	Prosody avant 0.9.4, lorsque mod_compression est activé, permet à des attaquants distants de provoquer un déni de service (consommation de ressources) via des éléments XML compressés dans un flux XMPP, aussi connu sous lâappellation dâattaque "zip bomb".	10/04/2014	4.3	CVE-2014-2750

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source Info & Correctif
qianqin -- qtranslate	Une vulnérabilité Cross-site request forgery (CSRF) dans le plugin qTranslate 2.5.34 et précédentes pour WordPress permet à des attaquants distants de détourner lâauthentification des administrateurs pour des requêtes qui changent les configurations du plugin via des vecteurs non spécifiés.	10/04/2014	6.8	CVE-2013-3251
redhat -- jboss_bpm_suite	JBoss Drools, Red Hat JBoss BRMS avant 6.0.1, et Red Hat JBoss BPM Suite avant 6.0.1 permet à des utilisateurs authentifiés à distance dâexécuter un code Java arbitraire via une expression (1) MVFLEX Expression Language (MVEL) ou (2) Drools.	10/04/2014	6.5	CVE-2013-6468
restful_web_services_project -- restws	Le module RESTful Web Services (RESTWS) 7.x-1.x avant 7.x-1.3 et 7.x-2.x avant 7.x-2.0-alpha5 pour Drupal, lorsque la mise en cache de la page est activée et des utilisateurs anonymes se sont vus attribués des permissions RESTWS, permet à des attaquants distants de provoquer un déni de service via une requête GET avec un entête HTTP Accept mis à type non-HTML, ce qui peut « interférer avec la page de cache de Drupal ».	06/04/2014	4.3	CVE-2013-1946
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 lâauthentification 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 Roundup avant 1.4.20 permet à des attaquants distants dâinjecter un script web ou HTML arbitraire via le paramètre otk.	10/04/2014	4.3	CVE-2012-6132
sap -- ccms_/_database_monitor	Une vulnérabilité non spécifiée dans SAP CCMS / Database Monitors pour Oracle permet à des attaquants dâobtenir le mot de passe de la base de données via des vecteurs inconnus.	10/04/2014	5.0	CVE-2013-7356
sap -- j2ee_engine	Une vulnérabilité non spécifiée dans le service de configuration dans SAP J2EE Engine permet à des	10/04/2014	5.0	CVE-2013-7357

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source Info & Correctif
	attaquants distants dôobtenir des informations dôauthentification via des vecteurs non spécifiés.			
sap -- guided_procedures_archive_monitor	Une vulnérabilité non spécifiée dans SAP Guided Procedures Archive Monitor permet à des attaquants distants dôobtenir les noms dôutilisateurs, les rôles, les profiles et éventuellement dôautres informations dôidentité via des vecteurs inconnus.	10/04/2014	5.0	CVE-2013-7358
sap -- mobile_infrastructure	Une vulnérabilité non spécifiée dans SAP Mobile Infrastructure permet à des attaquants distants dôobtenir des informations sensibles sur le port via des vecteurs inconnus, lié à un problème de « scannage interne de port ».	10/04/2014	5.0	CVE-2013-7359
sap -- cm_services	Une vulnérabilité traversée de répertoire dans SAP CMS et CM Services permet à des attaquants de transférer des fichiers arbitraires via des vecteurs non spécifiés.	10/04/2014	5.0	CVE-2013-7361
sap -- enterprise_portal	Une vulnérabilité Cross-site scripting (XSS) dans SAP Enterprise Portal permet à des attaquants distants dôinjecter un script web ou HTML arbitraire via des paramètres non spécifiés.	10/04/2014	4.3	CVE-2013-7365
sap -- software_deployment_manager	Le SAP Software Deployment Manager (SDM), dans certaines conditions non spécifiées, permet à des attaquants distants de provoquer un déni de service via des vecteurs lié aux authentifications échouées.	10/04/2014	5.0	CVE-2013-7366
sap -- hana	Le processus HANA ICM dans SAP HANA permet à des attaquants distants dôobtenir la version de la plateforme, le nom dôhôte, le numéro de lôinstance, et éventuellement dôautres informations sensibles via des requêtes HTTP GET malformées.	10/04/2014	5.0	CVE-2014-2749
silverstripe -- silverstripe	Une vulnérabilité Cross-site scripting (XSS) dans la fonction process dans SSViewer.php dans SilverStripe avant 2.3.13 et 2.4.x avant 2.4.6 permet à des attaquants distants dôinjecter un script web ou HTML arbitraire via QUERY_STRING vers le modèle placeholders, tel que démontré par une requête vers (1)	08/04/2014	4.3	CVE-2011-4958

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source Info & Correctif
	admin/reports/, (2) admin/comments/, (3) admin/, (4) admin/show/, (5) admin/assets/, and (6) admin/security/.			
tibco -- rendezvous	Rendezvous Daemon (rvd), Rendezvous Routing Daemon (rvrd), Rendezvous Secure Daemon (rvsd), et Rendezvous Secure Routing Daemon (rvsrd) dans TIBCO Rendezvous avant 8.4.2, Messaging Appliance avant 8.7.1, et Substation ES avant 2.8.1 nôimplémentent pas correctement un contrôle dâaccès, ce qui permet à des attaquants distants dôobtenir des informations sensibles ou modifier des informations transmises via des vecteurs non spécifiés.	08/04/2014	5.0	CVE-2014-2541
tibco -- rendezvous	Une vulnérabilité cross-site scripting (XSS) dans Rendezvous Daemon (rvd), Rendezvous Routing Daemon (rvrd), Rendezvous Secure Daemon (rvsd), et Rendezvous Secure Routing Daemon (rvsrd) dans TIBCO Rendezvous avant 8.4.2, Messaging Appliance avant 8.7.1, et Substation ES avant 2.8.1 permet à des attaquants distants dôinjecter un script web ou HTML arbitraire via des vecteurs non spécifiés.	08/04/2014	4.3	CVE-2014-2542
wordpress -- wordpress	WordPress avant 3.7.2 et 3.8.x avant 3.8.2 permet à des utilisateurs authentifiés à distance de publier des posts en utilisant le rôle de Contributor, lié à wp-admin/includes/post.php et wp-admin/includes/class-wp-posts-list-table.php.	09/04/2014	4.0	CVE-2014-0165
wordpress -- wordpress	La fonction wp_validate_auth_cookie dans wp-includes/pluggable.php dans WordPress avant 3.7.2 et 3.8.x avant 3.8.2 ne détermine pas correctement la validité de lâauthentification des cookies, ce qui rend plus facile pour des attaquants distants dôobtenir un accès via un cookie falsifié.	09/04/2014	6.4	CVE-2014-0166
wp-plugins -- wp-print	Une vulnérabilité Cross-site request forgery (CSRF) dans les options dans le plugin de WP-Print avant 2.52 pour WordPress permet à des attaquants distants de détourner lâauthentification des administrateurs pour des requêtes qui	10/04/2014	6.8	CVE-2013-2693

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source Info & Correctif
	manipulent les configurations du plugin via des vecteurs non spécifiés.			
znc -- znc-msvc	La fonction CBounceDCCMod::OnPrivCTCP dans bouncedcc.cpp dans le module bouncedcc dans ZNC 0.200 et 0.202 permet à des attaquants distants de provoquer un déni de service (crash) via une fausse requête DCC RESUME	08/04/2014	5.0	CVE-2012-0033

Retour haut de page

Vulnérabilités mineures

Editeur principal -- Produit	Description	Date de publication	Score CVSS	Source Info & Correctif
cloudbees -- jenkins	Une vulnérabilité Cross-site scripting (XSS) dans CloudBees Jenkins avant 1.514, LTS avant 1.509.1, et Enterprise 1.466.x avant 1.466.14.1 et 1.480.x avant 1.480.4.1 permet à des utilisateurs authentifiés à distance munis de permission dœcriture dœinjecter un script web ou HTML arbitraire via des vecteurs non spécifiés.	10/04/2014	2.1	CVE-2013-2033
gnu -- a2ps	La fonction tempname_ensure dans lib/routines.h dans a2ps 4.14 et antérieures, tel quœutilisé par la fonction spy_user et éventuellement dœautres fonctions, permet à des utilisateurs locaux de modifier des fichiers arbitraires via une attaque symlink sur un fichier temporaire.	05/04/2014	2.1	CVE-2001-1593

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