الجمهورية العربية السورية
الهيئة الوطنية لخدمات الشبكة
مركز أمن المعلومات

دليل الثغرات الأمنية في نظم تشغيل المخدّمات الخاصة بالمواقع الإلكترونية على شبكة الإنترنت

الإصدار الأول

دمشق في ٢٠١٢/٤/١٨

Tel: +963 11 3937032 Fax: +963 11 3937079 E-mail: isc@nans.gov.sy Website: www.nans.gov.sy

فهرس المحتويات

Tel: +963 11 3937032 Fax: +963 11 3937079 E-mail: isc@nans.gov.sy Website: www.nans.gov.sy

1. الثغرات الأمنية الموجودة في نظام التشغيل Ubuntu Linux:

إسم الثغرة	نوع الثغرة	الاصدارات المتأثرة	الوصف	عامل الخطورة	حزم التحديث
CVE-2011-3152	Update Manager vulnerabilities	Ubuntu 11.10 Ubuntu 11.04 Ubuntu 10.10 Ubuntu 10.04LTS Ubuntu 8.04LTS	تتسبب هذه الثغرة بتحميل التحديثات وتطبيقها قبل المصادقة ومطابقة التواقيع، مما قد يستغل من قبل المهاجمين بطريقة هجوم الرجل الذي في الوسط man-in-the-middle attack.	Medium	1
CVE-2011-3154	Update Manager vulnerabilities	Ubuntu 11.10 Ubuntu 11.04 Ubuntu 10.10 Ubuntu 10.04LTS Ubuntu 8.04LTS	قيام معالج التحديث بانشاء دليل (مجلد) مؤقت Temp بطريقة غير آمنة مما يسمح للمهاجمين بالاطلاع على معلومات خاصة بالمستخدم الذي يقوم بعملية بالتحديث الحالية	Medium	2
CVE-2011-3634	APT vulnerability	Ubuntu 11.04 Ubuntu 10.10 Ubuntu 10.04LTS Ubuntu 8.04 LTS	التعامل غير الصحيح مع خيار التحقق من الاتصال مما يسمح للمهاجمين بالنفاذ للنظام بسبب حصولهم على اتصال آمن بدل رفض الاتصال.	Medium	3
CVE-2011-3648	Thunderbird vulnerabilities	Ubuntu 11.10	ثغرة XSS في بعض النسخ القديمة نسبيا من المتصفحات Firefox, Thunderbird قد تسمح للمهاجمين بحقن شيفرات خبيثة عبر المتصفحات.	Medium	4
CVE-2011-3650	Thunderbird vulnerabilities	Ubuntu 11.10	عدم التعامل الصحيح مع ملفات Javascript والتي تحوي توابع متعددة قد تتسبب بالسماح للمهاجمين بالنفاذ الى ذاكرة النظام والتسبب بايقاف عمل التطبيقات وبالتالي اطلاق هجوم منع تقديم الخدمة DoS	Medium	5
CVE-2011-3651	Thunderbird vulnerabilities	Ubuntu 11.10	ثغرة في بعض النسخ القديمة نسبيا من المتصفحات Firefox, Thunderbird قد تسمح للمهاجمين بحقن شيفرات خبيثة عبر المتصفحات	Medium	6
CVE-2011-3652	Thunderbird vulnerabilities	Ubuntu 11.10	عدم التعامل الصحيح مع ذاكرة النظام اثناء تشغيل نسخ قديمة من المتصفحات Firefox,	Low	7

Tel: +963 11 3937032 Fax: +963 11 3937079 E-mail: isc@nans.gov.sy Website: www.nans.gov.sy

		Thunderbird مما قد يؤدي الى استغلال ذلك لاطلاق هجمة DoS			
8	Low	ثغرة في بعض النسخ القديمة نسبيا من المتصفحات Firefox, Thunderbird قد تسمح للمهاجمين بحقن شيفرات خبيثة عبر المتصفحات والتسبب بهجمة منع تقديم الخدمة.			CVE-2011-3654
9	Low	تسمح هذه الثغرة للمهاجمين بالحصول على بعض سماحيات النظام عن طريق بعض النسخ القديمة نسبيا من المتصفحات Firefox, Thunderbird.	Ubuntu 11.10	Thunderbird vulnerabilities	CVE-2011-3655
10	Medium	خلل في عمل الـ Kernel KSM Sharedpage Merging يؤدي استغلاله من قبل المهاجمين الى اطلاق هجمات DoS	Ubuntu 11.04	Linux (OMAP4) vulnerabilities	CVE-2011-2183
11	Medium	تتمثل هذه الثغرة في تابع mmap() وهو يستدعى من قبل الاجراء MAP_PRIVATE حيث يقوم التابع بانشاء عدد كبير من الصفحات والقوادح وذلك أثناء بعض عمليات الاختبار الخاصة بالنظام مما قد يستغل من قبل المهاجمين اطلاق هجمات DoS	Ubuntu 11.04	Linux (OMAP4) vulnerabilities	CVE-2011-2479
12	Medium	ثغرة في احد مكونات Linux kernel من جهة العميل client قد تسمح للمستخدمين المحليين غير المعرفين على النظام من اطلاق هجمات DoS	Ubuntu 11.04	Linux (OMAP4) vulnerabilities	CVE-2011-2491
13	Medium	تتمثل في عدم فرض النفاذ المقيد الى موارد النظام مما قد يسمح للمهاجم المحلي بالاطلاع على بعض المعلومات	Ubuntu 11.04	Linux (OMAP4) vulnerabilities	CVE-2011-2494
14	Medium	تتمثل في عدم فرض النفاذ المقيد الى موارد النظام مما قد يسمح للمهاجم المحلي بالاطلاع على بعض المعلومات	Ubuntu 11.04	Linux (OMAP4) vulnerabilities	CVE-2011-2495
15	Medium	استغلال هذه الثغرة سيؤدي الى أن	Ubuntu 11.04	Linux (OMAP4)	CVE-2011-2496

Tel: +963 11 3937032 Fax: +963 11 3937079 E-mail: isc@nans.gov.sy Website: www.nans.gov.sy

		المهاجم قد يستطيع اطلاق هجمات DoS من داخل الشبكة الداخلية		vulnerabilities	
16	Medium	ثغرة في ملفات تشغيل نظام الربط اللاسلكي مما قد يسمح للمستخدمين ذوي سماحية CAP_NET_ADMIN باطلاق هجمات DoS او كشف سماحياتهم عبر نظم الربط الشبكي الفعالة حينها	Ubuntu 11.04	Linux (OMAP4) vulnerabilities	CVE-2011-2517
17	Medium	ثغرة في اداة perf command تسمح للمستخدم العادي من خلال تشغيل بعض الاوامر العشوائية من اكتساب سماحيات متقدمة	Ubuntu 11.04	Linux (OMAP4) vulnerabilities	CVE-2011-2905
18	Low	تتمثل هذه الثغرة بخطأ برمجي في Comedi driver قد يتسبب بكشف معلومات من خلال الذاكرة leaked stack memory	Ubuntu 11.04	Linux (OMAP4) vulnerabilities	CVE-2011-2909
19	Medium	تُمكّن المهاجم من النفاذ الى CIFS Partition مما يؤدي إلى مشاكل في النظام بهجمات DoS	Ubuntu 11.04	Linux (OMAP4) vulnerabilities	CVE-2011-3363
20	Medium	تتعلق بـ mount.cifs بحيث قد يستطيع المستخدمون وبدون السماحيات المناسبة اجراء CIFS share mounted	Ubuntu 10.10	Linux (OMAP4) vulnerabilities	CVE-2011-1585
21	Medium	عدم قيام النظام باجراء التحقق من الادخال بالشكل المثالي عند معالجة ملفات archive files مما قد يسمح للمهاجمين بالتعديل والحذف على هذه الملفات	Ubuntu 11.10 Ubuntu 11.04 Ubuntu 10.10 Ubuntu 10.04 LTS	KDE Utilities vulnerability	CVE-2011-2725
22	Low	تتمثل هذه الثغرة بتسرب البيانات عند التعامل مع بيانات مشفرة ب TPM Trusted Platform Module مما قد يسمح للمستخدم غير المخول بقراءة البيانات من العملية السابقة لـ TPM	Ubuntu 11.10	Linux kernel vulnerability	CVE-2011-1162
23	Low	ثغرة في البروتوكول الخاص بالاداة Yahoo plugin الموجودة في برنامج المحادثة pidgin قد تؤدي الى امكانية اطلاق هجمة DoS من نوع Application crash	Ubuntu 11.04 Ubuntu 10.10 Ubuntu 10.04 LTS	Pidgin vulnerabilities	CVE-2011-1091

Tel: +963 11 3937032 Fax: +963 11 3937079 E-mail: isc@nans.gov.sy Website: www.nans.gov.sy

		قبل مهاجمين عبر الشبكات و من قبل مهاجمين عبر مخدمات Yahoo			
24	Low	ثغرة في البروتوكول الخاص بالاداة MSN plugin الموجودة في برنامج المحادثة pidgin قبل النسخة ٢,١٠,٠ قد تؤدي الى امكانية اطلاق هجمة DoS نوع incorrect memory access and application crash	Ubuntu 11.04 Ubuntu 10.10 Ubuntu 10.04 LTS	Pidgin vulnerabilities	CVE-2011-3184
25	Medium	ثغرة في البروتوكول الخاص بالاداة SILC protocol plugin الموجودة في البرنامج pidgin ومنتجات أخرى، قد تسمح بحدوث هجمات DoS من نوع crush	Ubuntu 11.04 Ubuntu 10.10 Ubuntu 10.04 LTS	Pidgin vulnerabilities	CVE-2011-3594
26	Medium	قد تتسبب بحدوث هجمات نوع DoS عند استقبال الرزم في حال تحميل وحدات ipip , ip_gre	Ubuntu 10.04 LTS	Linux kernel (FSL-IMX51) vulnerabilities	CVE-2011-1767
27	Medium	تتمثل في التعامل غير الصحيح للبروتوكول IP/IP مع بعض البيانات المرسلة عبر الشبكة، ان استغلال هذه الثغرة قد يسمح للمهاجم بإطلاق هجمات DoS	Ubuntu 10.04 LTS	Linux kernel (FSL-IMX51) vulnerabilities	CVE-2011-1768
28	High	عدم قدرة وحدة البرامج على التعرف والتحقق من شهادات المخدم server certificates مما قد يسمح للمهاجمين بتنفيذ شيفرات برمجية للحصول على المعلومات بطريقة هجوم الرجل في الوسط.	Ubuntu 11.10 Ubuntu 11.04 Ubuntu 10.10	Software Center vulnerability	CVE-2011-3150
29	Low	تتمثل هذه الثغرة بعيب في تطبيق الساعة الخاص بنواة النظام مما يؤدي إلى استغلالها من قبل المستخدمين المحليين غير المخولين بإطلاق هجمات DoS	Ubuntu 8.04 LTS	Linux kernel vulnerabilities	CVE-2011-3209
30	Medium	FreeType هي عبارة عن حزم برمجية تستخدم في عدد كبير من التطبيقات من أجل دعم الخطوط، الثغرة موجودة في النسخة FreeType2 تسمح للمهاجمين بتنفيذ شيفرات ماكرة واطلاق هجمات DoS نوع memory	Ubuntu 11.10 Ubuntu 11.04 Ubuntu 10.10 Ubuntu 10.04 LTS Ubuntu 8.04 LTS	FreeType vulnerabilities	CVE-2011-3256

Tel: +963 11 3937032 Fax: +963 11 3937079 E-mail: isc@nans.gov.sy Website: www.nans.gov.sy

		corruption			
31	Medium	خطأ في نسق تشفير المحارف UTF8 ضمن OpenLdap 2.4.26 وما قبل قد يسمح هذا الخطأ للمهاجمين باطلاق هجمات DoS نوع slapd crash	Ubuntu 11.10 Ubuntu 11.04 Ubuntu 10.10 Ubuntu 10.04 LTS	OpenLDAP vulnerability	CVE-2011-4079
32	High	يقوم system-config-printer (يستدعى بواسطة ملفات تشغيل الطباعة الافتراضية) باستخدام اتصال غير آمن للاتصال بقاعدة بيانات الطباعة OpenPrinting مما قد يسمح للمهاجمين باستخدام تقنية MITM	Ubuntu 11.10 Ubuntu 11.04	system-config-printer vulnerability	CVE-2011-4405
33	Medium	خطأ في البرنامج Bind 9.0 المستخدم في مخدم DNS قد يسمح للمهاجمين باطلاق هجمات Dos نوع assertion failure and named exit من خلال طلبات DNS العودية	Ubuntu 11.10 Ubuntu 11.04 Ubuntu 10.10 Ubuntu 10.04 LTS Ubuntu 8.04 LTS	Bind vulnerability	CVE-2011-4313
34	Medium	خطأ في Linux kernel2.6.32 وما قبل يتمثل بعدم معالجة الكم الكبير للعمليات المنفذة على فضاء عناوين الشبكة مما قد يسمح بحدوث هجمات DoS نوع memory consumption	Ubuntu 11.10 Ubuntu 11.04 Ubuntu 10.10 Ubuntu 10.04 LTS	vsftpd vulnerability	CVE-2011-2189
35	Medium	عدم قيام Light Display Manager بالتعامل الصحيح مع السماحيات وذلك لدى معالجة الملفات من النوع .dmrc مما قد يمكن المهاجمين من الاطلاع على بعض معلومات خصائص الملفات	Ubuntu 11.10	Light Display Manager vulnerabilities	CVE-2011-3153
36	Medium	عدم قيام Light Display Manager بالتعامل الصحيح مع الملفات links وذلك عند ضبط السماحيات الخاصة بالملفات من النوع Xauthority	Ubuntu 11.10	Light Display Manager vulnerabilities	CVE-2011-4105
37	Medium	تتعلق بعمل Quagga-Routing قبل النسخة 19.99 مع اللواحق غير الصحيحة لـ IPv6 بحيث	Ubuntu 11.10 Ubuntu 11.04 Ubuntu 10.10 Ubuntu 10.04 LTS	Quagga vulnerabilities	CVE-2011-3323

Tel: +963 11 3937032 Fax: +963 11 3937079 E-mail: isc@nans.gov.sy Website: www.nans.gov.sy

		يسمح للمهاجمين بإحداث هجمات DoS نوع out-of-bounds memory access and daemon crash			
38	Medium	التعامل غير الصحيح مع ملحقات IPv6 مما قد يؤدي الى هجمات DoS نوع assertion failure and daemon exit	Ubuntu 11.10 Ubuntu 11.04 Ubuntu 10.10 Ubuntu 10.04 LTS	Quagga vulnerabilities	CVE-2011-3324
39	Medium	تتعلق بعمل Quagga-Routing قبل النسخة 19.99 قد تسمح للمهاجمين باطلاق هجماتDoS نوع daemon crash من خلال ترويسة IPv4 أو جزء الترحيب في IPv6	Ubuntu 11.10 Ubuntu 11.04 Ubuntu 10.10 Ubuntu 10.04 LTS	Quagga vulnerabilities	CVE-2011-3325
40	Medium	تتعلق بعمل Quagga-Routing قبل النسخة 19.99 والتعامل مع رسائل تحديث IPv4 مما قد يتسبب بهجمات DoS نوع daemon crash	Ubuntu 11.10 Ubuntu 11.04 Ubuntu 10.10 Ubuntu 10.04 LTS	Quagga vulnerabilities	CVE-2011-3326
41	Medium	تتعلق بعمل Quagga-Routing قبل النسخة 19.99 والتعامل مع رسائل IPv4 مما قد يتسبب بهجمات DoS نوع daemon crash أو تنفيذ شيفرات خبيثة	Ubuntu 11.10 Ubuntu 11.04 Ubuntu 10.10 Ubuntu 10.04 LTS	Quagga vulnerabilities	CVE-2011-3327
42	Medium	عدم التعامل الصحيح لمخدم Apache مع RewriteRule و ProxyPassMatch مما قد يسمح للمهاجمين من خلال ارسال طلبات تحوي المحرف @ بالنفاذ الى مخدم الويب الداخلي	Ubuntu 11.10 Ubuntu 11.04 Ubuntu 10.10 Ubuntu 10.04 LTS Ubuntu 8.04 LTS	Apache vulnerabilities	
43	Medium	عند استخدام mod_proxy_ajp مع mod_proxy_balancer وفي ضبط معين قد تسمح هذه الظروف للمهاجمين باطلاق هجمات DoS نوع temporary "error state" in the backen server عن طريق طلبات http	Ubuntu 11.10 Ubuntu 11.04 Ubuntu 10.10 Ubuntu 10.04 LTS Ubuntu 8.04 LTS	Apache vulnerabilities	CVE-2011-3348
44	Medium	خطأ في عمل وحدة ITK Multi-Processing ضمن Apache وفي ظروف معينة تتسبب في منع مخدم Apache من التعامل	Ubuntu 11.10 Ubuntu 11.04 Ubuntu 10.10 Ubuntu 10.04 LTS Ubuntu 8.04 LTS	Apache vulnerabilities	CVE-2011-1176

Tel: +963 11 3937032 Fax: +963 11 3937079 E-mail: isc@nans.gov.sy Website: www.nans.gov.sy

		الصحيح مع سماحيات المستخدم مما قد يسمح للمهاجمين من النفاذ الى بعض سماحيات المستخدم root			
45	Medium	خطأ في برنامج مكافحة الفيروسات ClamAV يتعلق بالتعامل مع العودية recursion في ظروف معينة مما قد يسمح للمهاجم بإيقاف البرنامج اعتمادا على DoS نوع crush	Ubuntu 11.10 Ubuntu 11.04 Ubuntu 10.10 Ubuntu 10.04 LTS	ClamAV vulnerability	CVE-2011-3627
46	Medium	خطأ في radvd او Router Advertisement Daemon قد يمكن للمهاجمين استغلال ذلك من اجل ايقاف عمل radvd او محولة حقن وتنفيذ برمجيات خبيثة	Ubuntu 11.10 Ubuntu 11.04 Ubuntu 10.10 Ubuntu 10.04 LTS	radvd vulnerabilities	CVE-2011-3601
47	Medium	يتعلق بفلترة اسماء الواجهات interfaces عند انجاز عمليات انشاء بعض انواع الملفات مما قد يتسبب باعادة الكتابة على بعض الملفات	Ubuntu 11.10 Ubuntu 11.04 Ubuntu 10.10 Ubuntu 10.04 LTS	radvd vulnerabilities	CVE-2011-3602
48	Medium	خطأ في radvd او Router Advertisement Daemon يتعلق ببعض الأطوال مما قد يسمح للمهاجمين بإيقاف البرنامج اعتمادا على هجمات DoS	Ubuntu 11.10 Ubuntu 11.04 Ubuntu 10.10 Ubuntu 10.04 LTS	radvd vulnerabilities	CVE-2011-3604
49	Medium	خطأ في radvd او Router Advertisement Daemon في التعامل مع التأخير delay في حال الارسال المنفرد والذي قد يتسبب بتوقف البرنامج اعتمادا على هجمة DoS	Ubuntu 11.10 Ubuntu 11.04 Ubuntu 10.10 Ubuntu 10.04 LTS	radvd vulnerabilities	CVE-2011-3605
50	Low	ملف proc لا يقوم بتقييد النفاذ الى الدليل /proc بعد تنفيذ setuid program مما قد يسمح للمهاجمين بالنفاذ الى معلومات حساسة عن الملفات او تنفيذ DoS	Ubuntu 10.04 LTS	Linux kernel (Natty backport) vulnerabilities	CVE-2011-1020
51	Low	نظام Bluetooth لا يقوم بمسح الذاكرة بالشكل المطلوب مما قد يسمح للمهاجمين بقراءة ذاكرة نواة النظام	Ubuntu 10.04 LTS	Linux kernel (Natty backport) vulnerabilities	CVE-2011-1078

Tel: +963 11 3937032 Fax: +963 11 3937079 E-mail: isc@nans.gov.sy Website: www.nans.gov.sy

52	Medium	وجود عدة نقاط ضعف في تطبيق مصادقة HTTP DIGEST	Ubuntu 11.10 Ubuntu 11.04 Ubuntu 10.10 Ubuntu 10.04 LTS	Tomcat vulnerabilities	CVE-2011-1184
53	Medium	برتوكول خاص بـAJP في Apache Tomcat 7.0 قد يسمح للمهاجمين بانتحال طلبات AJP بدون مصادقة والحصول على معلومات حساسة	Ubuntu 11.10 Ubuntu 11.04 Ubuntu 10.10 Ubuntu 10.04 LTS	Tomcat vulnerabilities	CVE-2011-3190
54	Medium	ثغرة XSS	Ubuntu 11.10 Ubuntu 11.04 Ubuntu 10.10 Ubuntu 10.04 LTS	Empathy vulnerabilities	CVE-2011-3635
55	Medium	ثغرة XSS في النمط theme_adium_append_message في نسخ Empathy 3.2.1 وما قبل بحيث تسمح للمهاجمين بإمكانية حقن شيفرات برمجية او حتى HTML	Ubuntu 11.10 Ubuntu 11.04 Ubuntu 10.10 Ubuntu 10.04 LTS	Empathy vulnerabilities	CVE-2011-4170
56	Medium	تتمثل هذه الثغرة بكون اجرائية BackupPC تقوم بعملية فلترة الدخل وذلك عند معالجة رسالة خطأ في عرض ملف السجلات والذي قد يؤدي الى فتح ثغرة XSS	Ubuntu 11.10 Ubuntu 11.04 Ubuntu 10.10 Ubuntu 10.04 LTS Ubuntu 8.04 LTS	BackupPC vulnerabilities	CVE-2011-3361
57	Medium	عدم قدرة KDE-Libs وتحديدا KIO على تنفيذ عملية مصادقة وتحقق على الدخل وذلك عند التحقق من Proxy مما قد يسمح للمهاجمين بتعديل بعض بيانات العرض وحتى عنوان proxy	Ubuntu 11.04 Ubuntu 10.10 Ubuntu 10.04 LTS	KDE-Libs vulnerability	CVE-2011-3365
58	Medium	في نسخ kernel قبل 3.0 تسمح للمهاجمين باطلاق هجمات DoS نوع heap memory corruption	Ubuntu 11.04	Linux kernel vulnerabilities	CVE-2011-2497
59	Medium	في نسخ kernel قبل 2.6 وعندما يكون GRO فعالاً يقوم بعادة ضبط reset لبعض الحقول بطريقة غير صحيحة والذي قد يمكن المهاجمين من تنفيذ DoS نوع system crash	Ubuntu 11.04	Linux kernel vulnerabilities	CVE-2011-2723
60	Medium	معالجة linux kernel لعمليات توليد سلسلة أرقام عشوائية بطريقة غير صحيحة تماماً مما قد يعطي	Ubuntu 11.04	Linux kernel vulnerabilities	CVE-2011-3188

Tel: +963 11 3937032 Fax: +963 11 3937079 E-mail: isc@nans.gov.sy Website: www.nans.gov.sy

			الفرصة للمهاجمين (بالتنبؤ) بسلسلة الأرقام وحقن بيانات		

عناوين حزم التحديث والتفاصيل الإضافية :

1. http://people.canonical.com/~ubuntu-security/cve/2011/CVE-2011-3152.html
2. http://people.canonical.com/~ubuntu-security/cve/2011/CVE-2011-3154.html
3. http://people.canonical.com/~ubuntu-security/cve/2011/CVE-2011-3634.html
4. http://people.canonical.com/~ubuntu-security/cve/2011/CVE-2011-3648.html
5. http://people.canonical.com/~ubuntu-security/cve/2011/CVE-2011-3650.html
6. http://people.canonical.com/~ubuntu-security/cve/2011/CVE-2011-3651.html
7. http://people.canonical.com/~ubuntu-security/cve/2011/CVE-2011-3652.html
8. http://people.canonical.com/~ubuntu-security/cve/2011/CVE-2011-3654.html
9. http://people.canonical.com/~ubuntu-security/cve/2011/CVE-2011-3655.html
10. http://people.canonical.com/~ubuntu-security/cve/2011/CVE-2011-2183.html
11. http://people.canonical.com/~ubuntu-security/cve/2011/CVE-2011-2479.html
12. http://people.canonical.com/~ubuntu-security/cve/2011/CVE-2011-2491.html
13. http://people.canonical.com/~ubuntu-security/cve/2011/CVE-2011-2494.html
14. http://people.canonical.com/~ubuntu-security/cve/2011/CVE-2011-2495.html
15. http://people.canonical.com/~ubuntu-security/cve/2011/CVE-2011-2496.html
16. http://people.canonical.com/~ubuntu-security/cve/2011/CVE-2011-2517.html
17. http://people.canonical.com/~ubuntu-security/cve/2011/CVE-2011-2905.html
18. http://people.canonical.com/~ubuntu-security/cve/2011/CVE-2011-2909.html
19. http://people.canonical.com/~ubuntu-security/cve/2011/CVE-2011-3363.html
20. http://people.canonical.com/~ubuntu-security/cve/2011/CVE-2011-1585.html
21. http://people.canonical.com/~ubuntu-security/cve/2011/CVE-2011-2725.html
22. http://people.canonical.com/~ubuntu-security/cve/2011/CVE-2011-1162.html
23. http://people.canonical.com/~ubuntu-security/cve/2011/CVE-2011-1091.html
24. http://people.canonical.com/~ubuntu-security/cve/2011/CVE-2011-3184.html
25. http://people.canonical.com/~ubuntu-security/cve/2011/CVE-2011-3594.html
26. http://people.canonical.com/~ubuntu-security/cve/2011/CVE-2011-1767.html
27. http://people.canonical.com/~ubuntu-security/cve/2011/CVE-2011-1768.html
28. http://people.canonical.com/~ubuntu-security/cve/2011/CVE-2011-3150.html
29. http://people.canonical.com/~ubuntu-security/cve/2011/CVE-2011-3209.html
30. http://people.canonical.com/~ubuntu-security/cve/2011/CVE-2011-3256.html
31. http://people.canonical.com/~ubuntu-security/cve/2011/CVE-2011-4079.html
32. http://people.canonical.com/~ubuntu-security/cve/2011/CVE-2011-4405.html
33. http://people.canonical.com/~ubuntu-security/cve/2011/CVE-2011-4313.html
34. http://people.canonical.com/~ubuntu-security/cve/2011/CVE-2011-2189.html
35. http://people.canonical.com/~ubuntu-security/cve/2011/CVE-2011-3153.html
36. http://people.canonical.com/~ubuntu-security/cve/2011/CVE-2011-4105.html
37. http://people.canonical.com/~ubuntu-security/cve/2011/CVE-2011-3323.html
38. http://people.canonical.com/~ubuntu-security/cve/2011/CVE-2011-3324.html
39. http://people.canonical.com/~ubuntu-security/cve/2011/CVE-2011-3325.html
40. http://people.canonical.com/~ubuntu-security/cve/2011/CVE-2011-3326.html
41. http://people.canonical.com/~ubuntu-security/cve/2011/CVE-2011-3327.html

Tel: +963 11 3937032 Fax: +963 11 3937079 E-mail: isc@nans.gov.sy Website: www.nans.gov.sy

42. http://people.canonical.com/~ubuntu-security/cve/2011/CVE-2011-3368.html
43. http://people.canonical.com/~ubuntu-security/cve/2011/CVE-2011-3348.html
44. http://people.canonical.com/~ubuntu-security/cve/2011/CVE-2011-1176.html
45. http://people.canonical.com/~ubuntu-security/cve/2011/CVE-2011-3627.html
46. http://people.canonical.com/~ubuntu-security/cve/2011/CVE-2011-3601.html
47. http://people.canonical.com/~ubuntu-security/cve/2011/CVE-2011-3602.html
48. http://people.canonical.com/~ubuntu-security/cve/2011/CVE-2011-3604.html
49. http://people.canonical.com/~ubuntu-security/cve/2011/CVE-2011-3605.html
50. http://people.canonical.com/~ubuntu-security/cve/2011/CVE-2011-1020.html
51. http://people.canonical.com/~ubuntu-security/cve/2011/CVE-2011-1078.html
52. http://people.canonical.com/~ubuntu-security/cve/2011/CVE-2011-1184.html
53. http://people.canonical.com/~ubuntu-security/cve/2011/CVE-2011-3190.html
54. http://people.canonical.com/~ubuntu-security/cve/2011/CVE-2011-3635.html
55. http://people.canonical.com/~ubuntu-security/cve/2011/CVE-2011-4170.html
56. http://people.canonical.com/~ubuntu-security/cve/2011/CVE-2011-3361.html
57. http://people.canonical.com/~ubuntu-security/cve/2011/CVE-2011-3365.html
58. http://people.canonical.com/~ubuntu-security/cve/2011/CVE-2011-2497.html
59. http://people.canonical.com/~ubuntu-security/cve/2011/CVE-2011-2723.html
60. http://people.canonical.com/~ubuntu-security/cve/2011/CVE-2011-3188.html

Tel: +963 11 3937032 Fax: +963 11 3937079 E-mail: isc@nans.gov.sy Website: www.nans.gov.sy

2. الثغرات الأمنية الموجودة في نظام التشغيل Red Hat Enterprise Linux:

إسم الثغرة	التاريخ	الوصف	عامل الخطورة	تفاصيل إضافية
CVE-2011-4694	2011-12-07	ثغرة في البرنامج Adobe flash player 11.1.102.55 قد تسمح للمهاجمين بتنفيذ شيفرات برمجية خبيثة من خلال ملفات .swf	High	1
CVE-2011-4693				2
CVE-2011-4688	2011-12-08	ثغرة في المتصفح Mozilla Firefox 8.0.1 قد تسمح للمهاجمين من كشف المستندات في ذاكرة المتصفح من خلال تنفيذ شيفرات javascript	Low	3
CVE-2011-4675	2011-03-14	ثغرة تجاوز في المجلد io/filesystem/filesystem.cc تتعلق بلعبة Online Widelands قد تسمح للمهاجمين تمرير شيفرات خبيثة من خلال المحرف .dot وذلك في المسار المستخدم للارسال الملفات في اللعبة التي تعتمد على الانترنت	Medium	4
CVE-2011-4674	2011-12-02	ثغرة من النوع SQL injection مع popup.php وذلك في Zabbix 1.8.3 قد تسمح للمهاجمين بتنفيذ شيفرات SQL من خلال البارامتر only_hostid	Medium	5
CVE-2011-4607	2011-12-12	ثغرة الأداة PuTTy والتي تستخدم من اجل عمليات النفاذ البعيد مثل Telnet قد تسمح للمهاجمين بالنفاذ الى الاجراء التنفيذي للاداة او الذاكرة الظاهرية التي تستخدمها الاداة	Medium	6
CVE-2011-4603	2011-12-11	فشل في معالجة برتوكول SILC لتشفير المحارف UTF-8 وذلك لدى استقبال عدد كبير ومتنوع من الرسائل والذي قد يؤدي الى التوقف	Medium	7
CVE-2011-4601	2011-12-08	عند استقبال عدد كبير ومتنوع من الرسائل من قبل البرنامج pidgin يفشل oscar protocol plugin في معالجة تشفير المحارف UTF-8 مما قد يؤدي الى توقف البرنامج	Medium	8
CVE-2011-4599	2011-12-09	مشكلة في ذاكرة buffer overfaow في معايير تشفير المحارف ICU والتي قد تسمح للمهاجمين باختراق مكتبة الـ ICU	Medium	9

Tel: +963 11 3937032 Fax: +963 11 3937079 E-mail: isc@nans.gov.sy Website: www.nans.gov.sy

10	Medium	ثغرة NULL pointer في Asterisk handled INFO مما قد يعطي المهاجمين فرصة إطلاق هجمات نوع DoS	2011-12-09	CVE-2011-4598
11	Unspecified	وتتعلق بمنع تجاوز المجلد واحد انواع هجمات potential directory traversal HTTP للتأكد من ان الملفات المضغوطة نوع .TAR آمنة قبل فك ضغطها تمهيدا لاستخدامها	2011-12-13	CVE-2011-4596
12		خطأ في نواة النظام من حيث التعامل مع المؤشر وتحديدا الغاء المرجعية بدون العودة الى توابع copy_from_user family of functions	2011-12-08	CVE-2011-4594
13	Medium	عدة مشاكل/أخطاء (ثغرات) تتعلق ببرنامج Moodle وهو عبارة عن برنامج تعليم عن بعد course management system(CMS) أو Learning Management Systems (LMS) الإصدارات المتأثرة : Moodle 2.1.3 Moodle 2.0.6 Moodle 1.9.15	2011-12-07	CVE-2011-4593 CVE-2011-4592 CVE-2011-459١ CVE-2011-459٠ CVE-2011-458٩ CVE-2011-458٨ CVE-2011-458٧ CVE-2011-458٦ CVE-2011-458٥ CVE-2011-458٤ CVE-2011-458٣

Tel: +963 11 3937032 Fax: +963 11 3937079 E-mail: isc@nans.gov.sy Website: www.nans.gov.sy

				CVE-2011-45٨٢
				CVE-2011-45٨١
14	Medium	ثغرة XSS في الـ EPP أو Platform للJBoss Enterprise Portal وفي حال استطاع المهاجم النفاذ عن طريق مستخدم قد دخل مسبقا الى EPP يستطيع عندها المهاجم تنفيذ شيفرات ويب خبيثة خلال الجلسة	2011-12-07	CVE-2011-4580
15	Medium	ثغرة في PHP 5.4.0beta2 على النظم 32- bit تسمح للمهاجمين بقراءة بيانات الذاكرة مع امكانية إطلاق هجمات نوع DoS وذلك ضمن ملفات JPEG	2011-11-29	CVE-2011-4566
16	Medium	ثغرة في ISC dhcpd قد تسمح للمهاجمين من خلال ارسال رزم طلب ايقاف عمل dhcpd في حال كان المخدم قد اعد لمعالجة العبارات بصيغة معاملات المقارنة	2011-12-07	CVE-2011-4539
17	High	ثغرة في JasPer تتمثل بفشل البرنامج في العمل بشكل صحيح مع الملفات JPEG2000. مشكلة ذاكرة من النوع heap buffer overflows بالنتيجة قد تسمح بقراءة وتنفيذ شيفرات برمجية تحكمية من المهاجمين	2011-10-20	CVE-2011-4517
18				CVE-2011-4516
19	Medium	ثغرة في Apache نوع integer overflow تتسبب بحجز ذاكرة buffer بحجم صغير ، واستدعاء too-small buffer والذي بدوره يمتلئ ببيانات المستخدم ويتسبب بفيض buffer overflow	2011-11-02	CVE-2011-4415
20				CVE-2011-3607
21	Medium	ثغرة في الطباعة الافتراضية system-config-printer والتي تستخدم من قبل خدمة تحميل ملفات. إن تشغيل الطباعة تتمثل بفتح اتصال غير امن مع قاعدة بيانات الطباعة تؤدي بالنتيجة الى تعديل الرزم من خلال تقنية MITM	2011-11-29	CVE-2011-4405
22	Medium	خطأ شهادة توقيع تقود الى اخطاء ذاكرة في المسار lighttpd تؤدي الى مشاكل في التحقق في بروتوكول HTTP قد يتمكن المهاجم من اطلاق هجمات DoS من خلال طلبات تحقق	2011-11-30	CVE-2011-4362

Tel: +963 11 3937032 Fax: +963 11 3937079 E-mail: isc@nans.gov.sy Website: www.nans.gov.sy

		خاصة HTTP		
23	High	ثغرة تتعلق بتطبيق Mojarra Sun والخاص بدعم تطبيقات JSF وبقراءته لبعض المتغيرات قد يسمح للمهاجمين بحقن رماز نوع EL expressions	2011-11-29	CVE-2011-4358
24	Medium	ثغرة في لغة البرمجة Python وضمن مجموعة CGI kit تؤدي الى اخطاء نوع CGI script error تمكن المهاجم من ادخال نمط خاص ينفذ من قبل التطبيق الحالي الذي يستخدم Python يؤدي الى توقف التطبيق عن العمل	2011-11-27	CVE-2011-4357
25	High	ثغرة في وهو احد تطبيقات Python client تمكن المهاجم من تنفيذ رمازات معينة من خلال ارسال رسالة بأحد ادوات الـ Celery	2011-11-28	CVE-2011-4356
26	Medium	منقح gdb أو GNU Debugger قد يقوم بتحميل ملفات غير موثوقة عند تعريف debug_gdb_scripts. والذي قد يتسبب باختراق سماحيات المستخدم الحالي من قبل المهاجمين	2011-12-06	CVE-2011-4355
27	Medium	ثغرة في OpenSSL 0.9.8g 32-bit قد تتسبب باسترجاع المفتاح الخاص لـ TLS server	2011-11-28	CVE-2011-4354
28	Medium	تتعلق بهجمة تجاوز المجلد واحدى انواع هجمات HTTP potential directory traversal وذلك في المسار Yaws	2011-11-25	CVE-2011-4350
29	Medium	عدم قيام التابع kvm_vm_ioctl_assign_device بالتحقق ما اذا كان المستخدم الحالي يملك السماحيات المناسبة مما قد يسمح للمستخدم بالتعامل مع اجهزة PCI بطريقة غير مرخصة	2011-11-22	CVE-2011-4347
30	Medium	ثغرة نوع XSS موجودة في المسار ' System 'Details' <= 'Details' => 'Custom Info' قد تسمح للمستخدمين بتنفيذ رمازات خبيثة	2011-09-28	CVE-2011-4346
31	Medium	ثغرة نوع XSS موجودة في Namazu وهو محرك بحث نصي ، قد تؤدي هذه الثغرة الى تنفيذ رمازات خبيثة او الاطلاع على معلومات HTTP cookie	2011-11-23	CVE-2011-4345

Tel: +963 11 3937032 Fax: +963 11 3937079 E-mail: isc@nans.gov.sy Website: www.nans.gov.sy

32 33 34	Medium	ثغرة في احد تطبيقات Apache وهو MyFaces2.0 والذي يدعم تطبيقات JavaServer حيث يستطيع المهاجمون حقن تعابير ورمازات خبيثة	2011-12-06	CVE-2011-4343
35	Medium	سماحيات ملف غير آمنة ضمن الخدمة OpenIPMI قد تسمح لمستخدم محلي بايقاف عمل بعض البرامج الفعالة	2011-10-03	CVE-2011-4339
36	Medium	خطأ في أحد ملفات النظام نوع الخطأ Corrupted File System قد يؤدي الى الى خطأ ذاكرة نوع Buffer Overflow	2011-11-21	VE-2011-4330
37	Medium	ثغرة أمنية في مشغلات الفلاش Shockwave Flash plug-in GNU flash movie player وذلك في ادارة ملفات Http cookies قد تسمح للمهاجمين بقراءة بعض المعلومات الحساسة	2011-11-21	CVE-2011-4328
38	Medium	خطأ امني في المسار ssh-keysign والذي يتعلق بالأداة OpenSSL بحيث قد يستغل هذا الخطأ من قبل المهاجمين من خلال الحصول على سماحيات غير نظامية	2011-11-21	CVE-2011-4327
39	High	ثغرة في Headroom وتحديدا في التابع udp6_ufo_fragment قد يتمكن المهاجم في حال استغلال هذه الثغرة من ايقاف النظام عن العمل	2011-11-21	CVE-2011-4326
40	Medium	ثغرة في مخدم Jabber server قد تسمح للمهاجمين ومن خلال ارسال رزمة خاصة للمخدم من جعل المعالج يدخل في حلقة infinite loop والذي سيؤدي بدوره الى اطلاق هجمة DoS	2011-11-21	CVE-2011-4320
41	Medium	ثغرة من النوع XSS في لغة البرمجة Ruby وذلك في المنهج Translate وذلك لدى التعامل مع دخل مستخدم نوع HTML قد تسمح هذه الثغرة للمهاجمين بتحميل وتنفيذ رمازات خبيثة من النوع HTML, web script	2011-11-18	CVE-2011-4319
42	Medium	ثغرة في المخدم Davecot وهو مخدم بريد الكتروني آمن عند اعدادات معينة (x509 certificate لم تجهز بشكل مناسب لمطابقة اسم النظام المضيف البعيد) قد تمكن هذه الثغرة المهاجمين من تنفيذ اسلوب MITM	2011-11-18	CVE-2011-4318

Tel: +963 11 3937032 Fax: +963 11 3937079 E-mail: isc@nans.gov.sy Website: www.nans.gov.sy

CVE-2011-4317	2011-11-23	مشاكل اضافية في حزمة تحديث الثغرة CVE-2011-3368 والتي تتعلق بـ reverse proxy bypass flaw	Medium	43
CVE-2011-4315	2011-11-17	خطأ فيض ذاكرة heap في مخدم DNS والذي يستخدم في proxy و fastcgi models حيث يستطيع المهاجم اطلاق هجمات القوة الشرسة brute-force	Medium	44
CVE-2011-4313	2011-12-13	خطأ من النوع DoS في DNS وتحديداً في Berkeley Internet Name Domain (BIND قد تستثمر من قبل المهاجمين بواسطة استعلامات خاصة نوع DNS queries	High	45

عناوين حزم التحديث والتفاصيل الإضافية :

1. https://bugzilla.redhat.com/show_bug.cgi?id=761223
2. https://bugzilla.redhat.com/show_bug.cgi?id=761216
3. https://bugzilla.redhat.com/show_bug.cgi?id=761550
4. https://bugzilla.redhat.com/show_bug.cgi?id=684924
5. https://bugzilla.redhat.com/show_bug.cgi?id=759591
6. https://bugzilla.redhat.com/show_bug.cgi?id=766865
7. https://bugzilla.redhat.com/show_bug.cgi?id=766446
8. https://bugzilla.redhat.com/show_bug.cgi?id=761517
9. https://bugzilla.redhat.com/show_bug.cgi?id=765812
10. https://bugzilla.redhat.com/show_bug.cgi?id=765776
11. https://bugzilla.redhat.com/show_bug.cgi?id=767236
12. https://bugzilla.redhat.com/show_bug.cgi?id=761646
13. https://bugzilla.redhat.com/show_bug.cgi?id=761248
14. https://bugzilla.redhat.com/show_bug.cgi?id=760845
15. https://bugzilla.redhat.com/show_bug.cgi?id=758413
16. https://bugzilla.redhat.com/show_bug.cgi?id=761265
17. https://bugzilla.redhat.com/show_bug.cgi?id=747726
18. https://bugzilla.redhat.com/show_bug.cgi?id=747726
19. https://bugzilla.redhat.com/show_bug.cgi?id=750935
20. https://bugzilla.redhat.com/show_bug.cgi?id=750935
21. https://bugzilla.redhat.com/show_bug.cgi?id=758374
22. https://bugzilla.redhat.com/show_bug.cgi?id=758624
23. https://bugzilla.redhat.com/show_bug.cgi?id=757980
24. https://bugzilla.redhat.com/show_bug.cgi?id=757542
25. https://bugzilla.redhat.com/show_bug.cgi?id=757651
26. https://bugzilla.redhat.com/show_bug.cgi?id=703238
27. https://bugzilla.redhat.com/show_bug.cgi?id=757909
28. https://bugzilla.redhat.com/show_bug.cgi?id=757181
29. https://bugzilla.redhat.com/show_bug.cgi?id=756084

Tel: +963 11 3937032 Fax: +963 11 3937079 E-mail: isc@nans.gov.sy Website: www.nans.gov.sy

30. https://bugzilla.redhat.com/show_bug.cgi?id=742050
31. https://bugzilla.redhat.com/show_bug.cgi?id=756348
32. https://bugzilla.redhat.com/show_bug.cgi?id=760692
33. https://issues.apache.org/jira/secure/attachment/12504807/MYFACES-3405-1.patch
34. http://www.jakobk.com/2011/11/jsf-value-expression-injection-vulnerability/
35. https://bugzilla.redhat.com/show_bug.cgi?id=742837
36. https://bugzilla.redhat.com/show_bug.cgi?id=755431
37. https://bugzilla.redhat.com/show_bug.cgi?id=755518
38. https://bugzilla.redhat.com/show_bug.cgi?id=755640
39. https://bugzilla.redhat.com/show_bug.cgi?id=755584
40. https://bugzilla.redhat.com/show_bug.cgi?id=755551
41. https://bugzilla.redhat.com/show_bug.cgi?id=755004
42. https://bugzilla.redhat.com/show_bug.cgi?id=754980
43. https://bugzilla.redhat.com/show_bug.cgi?id=756483
44. https://bugzilla.redhat.com/show_bug.cgi?id=754757
45. https://bugzilla.redhat.com/show_bug.cgi?id=754398

Tel: +963 11 3937032 Fax: +963 11 3937079 E-mail: isc@nans.gov.sy Website: www.nans.gov.sy

3. الثغرات الموجودة في نظم التشغيل مايكروسوفت :

Microsoft Windows Server 2008 R2 Itanium

Microsoft Windows Server 2003 SP2

إسم الثغرة	التاريخ	نوع الثغرة ------- نسخةالنظام	الوصـــــف	عامل الخطورة ١٠ -- ٠	تفاصيل إضافية مع حزم التحديث
CVE-2012-0013	2012-01-11		ثغرة نوع Incomplete blacklist في اعداد: Windows Packager configuration تسمح للمهاجمين بتنفيذ رمازات عشوائية انطلاقا من تطبيق ClickOnce application وهو احد تطبيقات .NET.	9.3	54
CVE-2012-0004	2012-01-13	Exec Code	ثغرة غير محددة في DirectX تسمح للمهاجمين بتنفيذ رمازات عشوائية انطلاقا من ملفات الوسائط Media تتعلق الثغرة ب: Quartz.dll, Qdvd.dll, closed captioning, Line21 DirectShow filter		55
CVE-2012-0003	2012-01-10		ثغرة في البرنامج الشهير Windows Media Player_Library وتحديدا في ملف الربط الحيوي winmm.dll تسمح للمهاجمين بتنفيذ رمازات عشوائية انطلاقا من ملفات الميديا MIDI		56
CVE-2012-0001	2012-01-11	Bypass	ثغرة في نواة النظام بحيث انها لا تستطيع تحميل structured exception handling tables بالشكل الامثل وهو احد أدوات بيئة .NET. مما يمكن المهاجمين من تجاوز اجراء التحقق الامني SafeSEH بواسطة تطبيقات Visual C++		57
CVE-2011-3417	2011-12-30	--	ثغرة في بيئة ASP.NET والمتضمنة في اطار العمل .NET. تتعلق بنماذج التحقق حيث لا تستطيع البيئة دعم المحتويات الفورية مما قد يسنح للمهاجمين روابط URL	9.3	1
CVE-2011-3416	2011-12-30	Bypass	ثغرة في بيئة ASP.NET والمتضمنة في اطار العمل .NET. تتعلق بنماذج التحقق بحيث قد تسمح للمستخدمين البعيدين (remote) بالنفاذ الى حسابات المستخدمين بشكل غير مرخص بواسطة ادخال اسم مستخدم crafted username	8.5	
CVE-2011-3415	2011-12-30	--	ثغرة في بيئة ASP.NET والمتضمنة في اطار العمل .NET. نوع open redirect تتعلق	6.8	

Tel: +963 11 3937032 Fax: +963 11 3937079 E-mail: isc@nans.gov.sy Website: www.nans.gov.sy

		بنماذج التحقق قد تسمح للمهاجمين باعادة توجيه المستخدمينل لاطلاق هجمات الاصطياد الكتروني phishing			
	7.8	ثغرة في بيئة ASP.NET والمتضمنة في اطار العمل .NET. في احد توابع التطبيق Hash تتعلق بخطأ في حساب قيم hash value لبعض المعاملات في النماذج مما قد يمنح المهاجمين الفرصة لاطلاق هجمات DoS نوع CPU consumption	DoS	2011-12-30	CVE-2011-3414
2	7.2	ثغرة في بيئة التشغيل client/server ضمن Win32 تتعلق بعدم التحقق من السماحيات اثناء تنفيذ بعض العمليات مما قد تسمح للمهاجمين بالحصول على سماحيات اعلى	+Priv	٢٠١١-١٢-١٤	CVE-2011-3408
3	9.3	ثغرة في البريد الالكتروني وبرنامج المحادثة الفورية Windows Mail و Windows Meeting Space تتعلق بمسار بحث غير آمن مما قد يسمح للمستخدمين المحليين بربح سماحيات عالية من خلال برمجيات خبيثة نوع Trojan horse DLL	+Priv ٢٠٠٨	٢٠١١-١١-٩	CVE-2011-2016
4	10	ثغرة integer overflow في تطبيق البروتوكول TCP/IP تسمح للمهاجمين بتنفيذ رمازات عشوائية بواسطة ارسال رزم UDP الى بعض المنافذ المغلقة	Exec Code Overflow	2011-11-09	CVE-2011-2013
5	7.2	ثغرة في Win32k.sys في kernel-mode drivers قد تسمح للمهاجمين بالحصول على سماحيات اضافية من خلال تطبيقات معينة تحمل ملفات تشغيل غير صحيحة incorrect driver object	+Priv	2011-10-20	CVE-2011-2011
6	7.1	خطأ Array index في Win32k.sys في kernel-mode drivers قد تسمح للمهاجمين باطلاق هجمات DoS نوع reboot من خلال أنواع خطوط معينة truetype	DoS ٢٠٠٨	2011-11-09	CVE-2011-2004
7	9.3	ثغرة Buffer overflow في Win32k.sys في kernel-mode drivers تسمح للمهاجمين بتنفيذ رمازات عشوائية من خلال ملفات نوع .fon.	Exec Code Overflow	2011-10-20	CVE-2011-2003
	4.7	عدم التعامل السليم مع خطوط truetype من قبل Win32k.sys في kernel-mode drivers مما قد يسمح للمستخدمين المحليين باطلاق هجمات DoS نوع system hang	DoS 2008	2011-12-14	CVE-2011-2002

Tel: +963 11 3937032 Fax: +963 11 3937079 E-mail: isc@nans.gov.sy Website: www.nans.gov.sy

8	9.3	عدة مسارات بحث غير موثوقة تسمح للمستخدمين المحليين بربح سماحيات اضافية من خلال برمجيات خبيثة نوع Trojan horse DLL وذلك في دليل العمل الحالي والذي سيبدو لمجلد يحوي ملفات نوع doc, rtf, txt	+Priv	2011-11-09	CVE-2011-1991
9	7.2	ثغرة في Win32k.sys في kernel-mode تتعلق بعدم القيام بالتحقق السليم من نمط الادخال مما يسمح للمستخدمين المحليين بالحصول على السماحيات التي تخولهم اطلاق هجمات DoS نوع NULL pointer dereference and system crash	+Priv DoS	2011-10-20	CVE-2011-1985
10	9.3	مسار بحث غير آمن في Windows Data Access Components تسمح للمستخدمين المحليين بربح سماحيات اضافية من خلال برمجيات خبيثة نوع Trojan horse DLL مشحونة بملفات نوع xlsx. وذلك في دليل العمل الحالي	+Priv ٢٠٠٨	2011-10-04	CVE-2011-1975
11	4.7	عدم القيام بعملية تحليل سليمة لمعلومات الملف file metadata من قبل نواة النظام kernel والذي يسمح للمستخدمين المحليين باطلاق هجمات DoS نوع reboot	DoS ٢٠٠٨	2011-09-21	CVE-2011-1971
12	7.2	ثغرة في winsrv.dll في زمن التشغيل client/server في Win32 تتعلق بعدم التأكد من السماحيات اثناء ارسال inter-process device-event messages مما قد يسمح للمهاجمين بربح السماحيات	+Priv	2011-10-04	CVE-2011-1967
13	7.1	ثغرة في Tcpip.sys ضمن رزمة TCP/IP تتعلق بعدم التعامل الصحيح مع الروابط نوع URL-based QoS مما يسمح للمهاجمين باطلاق هجمات DoS نوع reboot بواسطة روابط ترسل الى web server	DoS ٢٠٠٨	2011-10-04	CVE-2011-1965
14	4.3	عدم قيام البروتوكول MHTML بالتعامل السليم مع تنسيق MIME في مستند يعتمد لغة HTML مما يسمح للمهاجمين باطلاق هجمة نوع XSS	XSS	2011-09-06	CVE-2011-1894
15	٧,٢	win32k.sys في kernel-mode drivers يسمح للمستخدمين المحليين باكتساب سماحيات من خلال بعض التطبيقات التي تطلق NULL pointer dereference	+Priv 2008	2011-10-04	CVE-2011-1888 CVE-2011-1887

Tel: +963 11 3937032 Fax: +963 11 3937079 E-mail: isc@nans.gov.sy Website: www.nans.gov.sy

					CVE-2011-1885
16	7.2	ثغرة نوع Use-after-free في win32k.sys _ kernel-mode driver قد تسمح للمستخدمين المحليين بالحصول على سماحيات اضافية من خلال تطبيقات خاصة تعمل على ادارة ملفات تشغيل Drivers بطريقة غير نظامية	+Priv	٢٠١١-١٠-٤	CVE-2011-1884
					CVE-2011-1883
					CVE-2011-1882
		ثغرة في win32k.sys _ kernel-mode driver مما يسمح للمستخدمين المحليين بالحصول على السماحيات من خلال تطبيقات معينة تطلق NULL pointer dereference			CVE-2011-1881
					CVE-2011-1880
		ثغرة نوع Use-after-free في win32k.sys _ kernel-mode driver قد تسمح للمستخدمين المحليين بالحصول على سماحيات اضافية من خلال تطبيقات خاصة تعمل على ادارة ملفات تشغيل Drivers بطريقة غير نظامية			CVE-2011-1879
					CVE-2011-1878
			+Priv 2008		CVE-2011-1877
			+Priv		CVE-2011-1876
					CVE-2011-1875
					CVE-2011-1874
17	9.3	إن win32k.sys _ kernel-mode driver في منصات العمل نوع 64-bit لا تقوم بالتحقق السليم من المؤشرات Pointers أثناء تحليل الخطوط نوع OpenType مما قد يؤدي الى امكانية تنفيذ رمازات عشوائية من قبل المهاجمين من خلال ملفات نوع OpenType	Exec Code	٢٠١١-٩-٦	CVE-2011-1873

Tel: +963 11 3937032 Fax: +963 11 3937079 E-mail: isc@nans.gov.sy Website: www.nans.gov.sy

18	7.8	ثغرة في Tcpip.sys ضمن رزمة TCP/IP تسمح للمهاجمين باطلاق هجمات DoS نوع reboot بواسطة سلسلة رسائل نوع ICMP	DoS	2011-10-04	CVE-2011-1871
19	7.8	إن نظام Distributed File System (DFS) يسمح للمهاجمين عن طريق remote DFS servers باطلاق هجمات DoS نوع system hang بواسطة استجابة نوع referral response	DoS	2011-09-06	CVE-2011-1869
20	7.2	خطأ نوع Integer overflow في زمن التشغيل Client/Server قد يسمح للمهاجمين بربح سماحيات تخولهم اطلاق هجمات DoS نوع memory corruption وذلك بواسطة تطبيقات تطلق بيانات ذاكرة غير صحيحة	DoS Overflow +Priv Mem. Corr.	2011-10-04	CVE-2011-1284
		عدم التعامل بالشكل الأمثل مع الذاكرة ويقوم باستخدام مؤشرات نوع NULL pointer مما قد يسمح للمستخدمين المحليين باكتساب سماحيات تخولهم اطلاق هجمات DoS نوع memory corruption			CVE-2011-1282
		زمن التشغيل Client/Server في النظام Win32 لا يقوم بتقييد عدد واجهات consoles التابعة للاجراءات مما قد يسمح للمستخدمين بربيح سماحيات تخولهم اطلاق هجمات DoS نوع memory corruption			CVE-2011-1281
21	10	SMB client يسمح لمخدمات SMB البعيدة والمشغلة ضمن منصات Linux, Unix بتنفيذ رمازات عشوائية محملة بواسطة SMBv1 or SMBv2 response	Exec Code	2011-07-18	CVE-2011-1268
22	7.8	SMB server يسمح للمهاجمين البعيدين Remote attackers باطلاق هجمات DoS نوع system hang بواسطة طلبات نوع SMBv1 or SMBv2 request	DoS 2008	2011-11-23	CVE-2011-1267
23	7.2	إن الـ Ancillary Function Driver (AFD) في afd.sy لا تقوم بعملية تحقق سليمة في نمط ادخال المستخدم مما قد يسمح للمستخدمين المحليين باكتساب سماحيات بواسطة تطبيقات معينة	+Priv	2011-07-18	CVE-2011-1249
24	9.3	ثغرة نوع مسار بحث غير آمن في Active Accessibility component تسمح للمستخدمين المحليين بربح سماحيات اضافية من خلال Trojan horse DLL في دليل العمل		2011-11-09	CVE-2011-1247

Tel: +963 11 3937032 Fax: +963 11 3937079 E-mail: isc@nans.gov.sy Website: www.nans.gov.sy

		الحالي			
25	7.2	ثغرة نوع Use-after-free في win32k.sys _ kernel-mode driver قد تسمح للمستخدمين المحليين بالحصول على سماحيات اضافية من خلال تطبيقات خاصة تعمل على ادارة ملفات تشغيل Drivers بطريقة غير نظامية	+Priv	2011-10-04	CVE-2011-1242
					CVE-2011-1241
					CVE-2011-1240
					CVE-2011-1239
					CVE-2011-1238
					CVE-2011-1237
					CVE-2011-1236
					CVE-2011-1235
					CVE-2011-1234
					CVE-2011-1233
					CVE-2011-1232
					CVE-2011-1231
					CVE-2011-1230

Tel: +963 11 3937032 Fax: +963 11 3937079 E-mail: isc@nans.gov.sy Website: www.nans.gov.sy

25		ثغرة نوع Use-after-free في win32k.sys _ kernel-mode driver قد تسمح للمستخدمين المحليين بالحصول على سماحيات اضافية من خلال تطبيقات خاصة تعمل على ادارة ملفات تشغيل Drivers بطريقة غير نظامية		2011-10-04	CVE-2011-1229
					CVE-2011-1228
					CVE-2011-1227
					CVE-2011-1226
					CVE-2011-1225
					CVE-2011-0677
		ثغرة نوع Use-after-free في win32k.sys _ kernel-mode driver قد تسمح للمستخدمين المحليين بالحصول على سماحيات اضافية من خلال تطبيقات خاصة تعمل على ادارة ملفات تشغيل Drivers بطريقة غير نظامية			CVE-2011-0676
25	7.2	ثغرة نوع Use-after-free في win32k.sys _ kernel-mode driver قد تسمح للمستخدمين المحليين بالحصول على سماحيات اضافية من خلال تطبيقات خاصة تعمل على ادارة ملفات تشغيل Drivers بطريقة غير نظامية	+Priv	2011-10-04	CVE-2011-0675
					CVE-2011-0674
					CVE-2011-0672
					CVE-2011-0671
					CVE-2011-0670

Tel: +963 11 3937032 Fax: +963 11 3937079 E-mail: isc@nans.gov.sy Website: www.nans.gov.sy

					CVE-2011-0667
					CVE-2011-0666
					CVE-2011-0665
					CVE-2011-0662
26	10	إن مخدم SMB لا يقوم بعملية تحقق سليمة من الحقول المكونة لطلبات SMB مما قد يسمح للمهاجمين بتنفيذ رمازات عشوائية بواسطة رزم معدلة SMBv1 SMBv2		2011-10-04	CVE-2011-0661
27	9.3	خطأ في OLE Automation protocol implementation في VBscript.dll يسمح للمهاجمين بتنفيذ رمازات عشوائية من خلال ملفات windows Metafile WMF	Exec Code	2011-07-18	CVE-2011-0658
28	7.5	DNSAPI.dll في DNS client لا يتعامل بالشكل الأمثل مع الاستعلامات DNS queries مما قد يسمح للمهاجمين بتنفيذ رمازات عشوائية انطلاقا من استعلامات LLMNR broadcast		2011-10-04	CVE-2011-0657
29	4.3	عدم قيام البروتوكول MHTML بالتعامل السليم مع تنسيق MIME في مستند يعتمد لغة HTML مما يسمح للمهاجمين باطلاق هجمة نوع cross-site scripting وذلك بواسطة مواقع يتم طلبها بالمتصفح Internet Explorer	XSS	2011-10-04	CVE-2011-0096
30	6.4	نظام التحقق من الهوية Kerberos لا يمنع جلسة مستخدم حالية من التحول من نظام تشفير قوي الى نظام التشفير DES مما يمنح المهاجمين بطريقة الرجل الذي في الوسط فرصة التجسس على الرزم المارة عبر الشبكة والحصول على معلومات بواسطة التجسس على DES	+Info 2008	2011-07-18	CVE-2011-0091
31	9.3	خطأ فيض ذاكرة نوع overflow في ملفات تشغيل تنسيقات الخطوط OpenType CFF مما يسمح للمهاجمين بتنفيذ رمازات عشوائية بواسطة قيم معينة لبارامترات في خطوط OpenType	Exec Code Overflow	2011-10-04	CVE-2011-0034

Tel: +963 11 3937032 Fax: +963 11 3937079 E-mail: isc@nans.gov.sy Website: www.nans.gov.sy

32	7.1	JScript 5.8 و VBScript 5.8 لا تقوم بتحميل المخطوط البرمجي المستخرج من صفحات الويب بالشكل الامثل مما قد يسمح للمهاجمين باختراق الذاكرة وبالتالي الحصول على معلومات هامة وذلك بواسطة صفحات ويب معينة	Mem. Corr. +Info	2011-07-18	CVE-2011-0031
33	9.3	ثغرة مسار بحث غير آمن في تطبيق الاتصال Microsoft Remote Desktop 5.2, 6.0, 6.1, 7.0 من طرف العميل قد تسمح للمستخدم المحلي بريح سماحيات اضافية بواسطة ملف تروجان dll. في دليل العمل الحالي تظهر على شكل مجلد يحوي ملف rdp.	+Priv	2011-10-04	CVE-2011-0029
34	7.2	مشكلة فيض ذاكرة نوع buffer-overflow في التابع RtlQueryRegistryValues في النظام win32k.sys تسمح للمستخدم المحلي باكتساب سماحيات اضافية وتجاوز ميزة حساب المستخدم User Account Control (UAC) بواسطة قيم ثنائية لمسجل النظام REG_BINARY للمفتاح SystemDefaultEUDCFont	Overflow +Priv Bypass	2011-07-18	CVE-2010-4398
35	7.6	ثغرة في محرر الصفحة الأولى للفاكس وتحديدا الملف التنفيذي fxscover.exe والتي لاتقوم بتحليل parse صفحات الفاكس الأولى بالشكل الامثل مما قد يسمح للمهاجمين بتنفيذ رمازات عشوائية بواسطة ملفات نوع cov.	Exec Code Overflow Mem. Corr.	2011-10-04	CVE-2010-3974
36	9.3	مسار بحث غير آمن في حال كانت ميزة BranchCache مدعومة كما في Windows7, windows server2008 يسمح للمستخدم المحلي بزيادة السماحيات من خلال Trojan horse DLL في دليل العمل الحالي مخفية في مجلد يحوي ملفات نوع EML, RSS, WPOST	+Priv ٢٠٠٨	2011-07-28	CVE-2010-3966
37	7.2	مشكلة في User Interface (UI) بحيث لا يستطيع النظام التعامل مع قيم مفاتيح مسجل النظام الغير المحددة مما يسمح للمستخدم المحلي باكتساب سماحيات اضافية من خلال SeImpersonatePrivilege rights		2011-07-18	CVE-2010-3961
38		ثغرة في Win32k.sys في kernel-mode تتعلق بعدم التحقق من نمط ادخال المستخدم مما قد يسمح للمستخدمين بالحصول على سماحيات اضافية بواسطة تطبيقات معينة	+Priv Mem. Corr. 2008		CVE-2010-3944

Tel: +963 11 3937032 Fax: +963 11 3937079 E-mail: isc@nans.gov.sy Website: www.nans.gov.sy

39		ثغرة في مجدول المهام Scheduler بحيث لا يقوم بالاخذ بعين الاعتبار السياق الامني للمهمة المجدولة مما قد يسمح للمستخدمين بالحصول على سماحيات اضافية	+Priv ٢٠٠٨		CVE-2010-3338
40	7.1	ثغرة في الحزمة الامنية Security Channel عند استخدام النسخ 7.x من المخدم IIS حيث لا تقوم القناة الآمنة بالمعالجة الصحيحة لشهادة العميل اثناء عمليات تبادل الشهادات نوعي SSL, TLS والذي قد يمكن المهاجمين من اطلاق هجمات منع تقديم الخدمة نوع LSASS outage and reboot	DoS ٢٠٠٨	2011-10-04	CVE-2010-3229
41	7.5	ان واجهة المستخدم الخاصة بخدمة عناقيد المخدمات Cluster Service لا تقوم بعملية اسناد صحيحة لسماحية administrative-share للاقراص الجديدة مما قد يسمح للمهاجمين من قراءة او حنى تعديل االبيانات على هذه الاقراص من خلال هذه السماحية	-- ٢٠٠٨	2011-07-18	CVE-2010-3223
42	7.6			2011-10-04	CVE-2010-2746
43	9.3	ثغرة في خدمة رتل الطباعة Print spooler عند تفعيل المشاركة في الطباعة لا تقوم بالتحقق الكافي من سماحيات المشاركة في الطباعة مما يمكن المهاجمين من انشاء ملفات ضمن مجلد النظام وتنفيذ رمازات عشوائية بواسطة ارسال طلبات طباعة بواسطة الاجراء RPC	Exec Code	2011-07-18	CVE-2010-2729
44		ثغرة في واجهة النظام Windows shell يسمح للمستخدمين المحليين والمهاجمين البعيدين بتنفيذ رمازات عشوائية بواسطة ملفات نوع اختصارات .PIF, .LNK والتي (الملفات) لا يتم التعامل معها بالشكل الامثل من قبل برنامج Windows explorer		2011-03-10	CVE-2010-2568
45	6.8	يمكن للمستخدمين اكتساب سماحيات اضافية بواسطة للاجراءات من خلال اجراءات خدمة NetworkService مثل: TAPI server, SQL server, IIS,	+Priv	2010-08-17	CVE-2010-1886
46	9.3	خطأ ذاكرة نوع Integer overflow في محرك الخطوط المضمن مع النظام Embedded OpenTypeيسمح للمهاجمين بتنفيذ رمازات عشوائية	Exec Code Overflow	2011-10-04	CVE-2010-1883

Tel: +963 11 3937032 Fax: +963 11 3937079 E-mail: isc@nans.gov.sy Website: www.nans.gov.sy

47	6.8	win32k.sys في kernel-mode drivers يسمح للمستخدمين بتنفيذ رمازات عشوائية	Exec Code	2010-08-21	CVE-2010-1255
48	7.2	ثغرة غير محددة في مشغل الخطوط نوع OpenType Compact Font Format تسمح للمستخدمين بتنفيذ رمازات عشوائية مستغلين عدم التحقق المناسب اثناء نسخ البيانات من user mode الى kernel mode	Exec Code Overflow		CVE-2010-0819
49	9.3	عدة ثغرات غير محددة في المتصفح Internet Explorer8 تتعلق بادوات التطوير والتحكم بعناصر ActiveX قد تسمح هذه الثغرات للمهاجمين بتنفيذ رمازات خبيثة	Exec Code	2011-07-18	CVE-2010-0811
50	6.8	win32k.sys في kernel-mode drivers لا يقوم بالتحقق من بعض المتغيرات اثناء انشاء النوافذ مما يسمح للمستخدمين بتنفيذ رمازات خبيثة		2010-08-21	CVE-2010-0485
51 52	9.3	ثغرة في Data Analyzer ActiveX control في مكتبة الربط الحيوي max3activex.dll تسمح للمهاجمين بتنفيذ رمازات عشوائية من خلال صفحات ويب معينة	Exec Code	2010-08-21	CVE-2010-0252
53	9.3	خطأ ذاكرة نوع Heap-based buffer overflow في DirectX حيث يستخدم كفلتر لملفات AVI. تسمح للمهاجمين بتنفيذ رمازات خبيثة انطلاقا من ملفات نوع AVI.	Exec Code Overflow	2011-01-06	CVE-2010-0250

عناوين حزم التحديث وتفاصيل إضافية أخرى :

1. http://technet.microsoft.com/security/bulletin/MS11-100
2. http://technet.microsoft.com/security/bulletin/MS11-097
3. http://technet.microsoft.com/security/bulletin/MS11-085
4. http://technet.microsoft.com/security/bulletin/MS11-083
5. http://technet.microsoft.com/en-us/security/bulletin/MS11-077
6. http://technet.microsoft.com/security/bulletin/MS11-084
7. http://technet.microsoft.com/en-us/security/bulletin/MS11-077
8. http://technet.microsoft.com/en-us/security/bulletin/MS11-071
9. http://technet.microsoft.com/en-us/security/bulletin/MS11-077
10. http://www.microsoft.com/technet/security/bulletin/ms11-059.mspx
11. http://www.microsoft.com/technet/security/bulletin/ms11-068.mspx
12. http://www.microsoft.com/technet/security/bulletin/ms11-063.mspx
13. http://www.microsoft.com/technet/security/bulletin/ms11-064.mspx
14. http://www.microsoft.com/technet/security/bulletin/ms11-037.mspx

Tel: +963 11 3937032 Fax: +963 11 3937079 E-mail: isc@nans.gov.sy Website: www.nans.gov.sy

15. http://www.microsoft.com/technet/security/bulletin/ms11-054.mspx
16. http://www.microsoft.com/technet/security/bulletin/ms11-054.mspx
17. http://www.microsoft.com/technet/security/bulletin/ms11-041.mspx
18. http://www.microsoft.com/technet/security/bulletin/ms11-064.mspx
19. http://www.microsoft.com/technet/security/bulletin/ms11-042.mspx
20. http://www.microsoft.com/technet/security/bulletin/ms11-056.mspx
21. http://www.microsoft.com/technet/security/bulletin/ms11-043.mspx
22. http://www.microsoft.com/technet/security/bulletin/ms11-048.mspx
23. http://www.microsoft.com/technet/security/bulletin/ms11-046.mspx
24. http://technet.microsoft.com/en-us/security/bulletin/MS11-075
25. http://www.microsoft.com/technet/security/bulletin/ms11-034.mspx
26. http://www.microsoft.com/technet/security/bulletin/ms11-020.mspx
27. http://www.microsoft.com/technet/security/bulletin/ms11-038.mspx
28. http://www.microsoft.com/technet/security/bulletin/ms11-030.mspx
29. http://www.microsoft.com/technet/security/bulletin/ms11-026.mspx
30. http://www.microsoft.com/technet/security/bulletin/ms11-013.mspx
31. http://www.microsoft.com/technet/security/bulletin/ms11-032.mspx
32. http://www.microsoft.com/technet/security/bulletin/ms11-009.mspx
33. http://www.microsoft.com/technet/security/bulletin/ms11-017.mspx
34. http://www.microsoft.com/technet/security/bulletin/ms11-011.mspx
35. http://www.microsoft.com/technet/security/bulletin/ms11-024.mspx
36. http://www.microsoft.com/technet/security/bulletin/ms10-095.mspx
37. http://www.microsoft.com/technet/security/bulletin/ms10-100.mspx
38. http://www.microsoft.com/technet/security/bulletin/ms10-098.mspx
39. http://www.microsoft.com/technet/security/bulletin/ms10-092.mspx
40. http://www.microsoft.com/technet/security/bulletin/ms10-085.mspx
41. http://www.microsoft.com/technet/security/bulletin/ms10-086.mspx
42. http://www.microsoft.com/technet/security/bulletin/ms10-081.mspx
43. http://www.microsoft.com/technet/security/bulletin/ms10-061.mspx
44. http://www.microsoft.com/technet/security/bulletin/ms10-046.mspx
45. http://www.microsoft.com/technet/security/advisory/2264072.mspx
46. http://www.microsoft.com/technet/security/bulletin/ms10-076.mspx
47. http://www.microsoft.com/technet/security/bulletin/ms10-032.mspx
48. http://www.microsoft.com/technet/security/bulletin/ms10-037.mspx
49. http://www.microsoft.com/technet/security/bulletin/ms10-034.mspx
50. http://www.microsoft.com/technet/security/bulletin/ms10-032.mspx
51. http://www.microsoft.com/technet/security/bulletin/ms10-034.mspx
52. http://www.microsoft.com/technet/security/bulletin/ms10-008.mspx
53. http://www.microsoft.com/technet/security/bulletin/ms10-013.mspx
54. http://technet.microsoft.com/security/bulletin/MS12-005
55. http://technet.microsoft.com/security/bulletin/MS12-004
56. http://technet.microsoft.com/security/bulletin/MS12-004
    http://technet.microsoft.com/security/bulletin/MS12-001

Tel: +963 11 3937032 Fax: +963 11 3937079 E-mail: isc@nans.gov.sy Website: www.nans.gov.sy

3. الثغرات الأمنية الموجودة في نظام التشغيل Debian Linux:

إسم الثغرة	التاريخ	التصنيف	الوصف	عامل الخطورة	تفاصيل إضافية
CVE-2012-0050	23-1-2012	DSA-2392-1 openssl -- out-of-bounds read	برمجيات التأمين OpenSSL 0.9.8s/ 1.0.0f لا تدعم تطبيقات DTLS مما قد يسمح للمهاجمين البعيدين بتنفيذ هجمات DoS	Medium	42
CVE-2011-2930		DSA-2301-2 rails	ثغرة نوع SQL injection في المنهج quote_table_name في البيئة Ruby في Rails قبل 2.3.13 وقبل 3.0.10 وقبل 3.1.0.rc5 تسمح للمهاجمين بتنفيذ تعليمات SQL عشوائية من خلال اسم الحقل	High	43
CVE-2011-2931			ثغرة نوع XSS في strip_tags: help في البيئة Ruby في Rails قبل 2.3.13 وقبل 3.0.10 وقبل 3.1.0.rc5 تسمح للمهاجمين بحقن رمازات HTML او رمازات Web scripts	Medium	44
CVE-2011-3186			ثغرة نوع CRLF injection في actionpack/lib/action_controller/response.rb في البيئة Ruby في Rails الاصدارات 2.3.x وقبل 2.3.13 حيث تسمح للمهاجمين بحقن ترويسات HTTP عشوائية		45
CVE-2009-4214			ثغرة نوع XSS في التابع strip_tags والمتضمن في البيئة Ruby في Rails النسخ 2.2.s/2.3.x قبل 2.3.5 تسمح للمهاجمين بحقن رمازات عشوائية نوع web script / HTML بواسطة محارف نوع non-printing ASCII		46
CVE-2011-1940	22-1-2012	DSA-2391-1 phpmyadmin	مشكلة في اداة الادارة phpMyAdmin XSS محاملة في الميزة table tracking تسمح للمهاجمين بحقن رمازات عشوائية نوع web script / HTML	Unspecified	47
CVE-2011-3181			ثغرة نوع XSS في اداة التعقب في phpMyAdmin النسخ 3.3.x— 3.3.10.4 / 3.4.x—3.4.4 تسمح للمهاجمين بحقن رمازات عشوائية نوع web script / HTML	Medium	48

Tel: +963 11 3937032 Fax: +963 11 3937079 E-mail: isc@nans.gov.sy Website: www.nans.gov.sy

49		تابع simplexml_load_string في الاداة المضمنة في libraries/import/xml.php phpMyAdmin 3.4.x & 3.4.7.1 & 3.3.x & 3.3.10.5 تسمح للمستخدمين االبعيدين المخولين بقراءة ملفات XML			CVE-2011-4107
1	Medium	تطبيق DTLS implementation في اداة تبادل الشهادات OpenSSL قبل النسخة 0.9.8s وقبل النشخة 1.0.0f تقوم بعملية مطابقة للعنوان الفيزيائي MAC فقط في حال وجود Padding معين مما يسمح للمهاجمين بكشف نصوص غير مشفرة بواسطة padding oracle attack	DSA-2390 openssl	٢٠١٢-١-١٥	CVE-2011-4108
2	High	ثغرة مزدوجة في OpenSSL قبل 0.9.8s عندما تكون ميزة X509_V_FLAG_POLICY_CHECK في وضع التفعيل تسمح للمهاجمين بالقيام بهجمة مستغلين فشل التحقق من السياسة.			CVE-2011-4109
3	Medium	في منصات عمل 32-bit –عمليات التشفير نوع NIST elliptic curves P-256 P-384 لا تقوم بالعمل بشكل صحيح بحيث هناك ضعف في المفتاح الخاص ECC وذلك في مخدمات TLS			CVE-2011-4354
4		تطبيق SSL 3.0 في OpenSSL قبل النسخة 0.9.8s وقبل 1.0.0f لا تقوم بالتمييز الصحيح للبيانات لبلوك التشفير والذي يسمح للمهاجمين بالحصول على معلومات هامة بواسطة عملية فك التشفير			CVE-2011-4576
5		تطبيق المخدم SGC في OpenSSL قبل النسخة 0.9.8s وقبل 1.0.0f لا تقوم بالتعامل الصحيح مع اعادة تشغيل عمليات المطابقة المباشرة handshake مما يسمح للمهاجمين بهجمات نوع DoS			CVE-2011-4619
6	Medium	مشكلة تتعلق ب KSM وهو عبارة عن اداة لتنظيم استخدام الذاكرة بحيث يستطيع المستخدم من خلال استغلال الاجراءات الخارجة من الذاكرة اطلاق بهجمات DoS نوع Kernel oops	DSA-2389 linux-2.6 privilege escalation/denial of service/information leak	٢٠١٢-١-١٥	CVE-2011-2183

Tel: +963 11 3937032 Fax: +963 11 3937079 E-mail: isc@nans.gov.sy Website: www.nans.gov.sy

7	Medium	ثغرة في kernel قبل2.6.39.3 تتعلق بالتابع inet_diag_bc_audit والموجود في الحزمة net/ipv4/inet_diag.c لا يقوم بعمل تتبع صحيح لـINET_DIAG bytecode مما يسمح للمستخدمين المحليين بالتسبب بمشكلة kernel infinite loop وبالنتيجة اطلاق DoS			CVE-2011-2213
8	Low	ثغرة ضعف في الأداة packet socket implementation			CVE-2011-2898
9	Medium	ثغرة في FUSE وهو مصطلح يمثل نظام الملفات في مساحة عمل المستخدم حيث من الممكن حدوث DoS نوع buffer overflow بواسطة المستخدمين المحليين	DSA-2389 linux-2.6 privilege escalation/denial of service/information leak	٢٠١٢-١-١٥	CVE-2011-3353
10	High	مشكلة في نظام الملفات XFS حيث يستطيع مستخدم محلي يتمتع بسماحية Mount لملفات النظام التسبب بنتيجة Corruoption Memory واكتساب المزيد من السماحيات			CVE-2011-4077
11	Medium	مشكلة في النظام kernel's access key retention تسمح للمستخدمين بالتسبب بـ kernel infinite loop وبالنتيجة اطلاق DoS			CVE-2011-4110
12	High	مشكلة في التطبيق IOcontrol: IOCTLpassthrough والذي يدعم تجهيزات SCSI فالمستخدم الذي يملك سماحية النفاذ الى قسم منطقي من القرص يستطيع النفاذ الى كامل الجهاز بواسطة المسار SG_IO ioctl			CVE-2011-4127
13	Medium	خطأ في الأداة PERF وهي اداة لتحليل أداء نظم Linux وتحديدا العاملة منها على نظم POWER7 Systems قد تسمح للمستخدمين المحليين اطلاق بجمات DoS			CVE-2011-4611
14	Medium	مشكلة في اداة KVM PIT Timer Kernel-based Virtual Machine حيث يستطيع المستخدم المحلي مع سماحية على الKVM التسبب بهجمة			CVE-2011-4622

Tel: +963 11 3937032 Fax: +963 11 3937079 E-mail: isc@nans.gov.sy Website: www.nans.gov.sy

		DoS من خلال البدء بعداد PIT بدون تجهيز irqchip			
15	High	عدة مشاكل في برتوكول ROSE protocol قد يستغل المستخدم البعيد هذه الثغرات للوصول الى اماكن حساسة في الذاكرة والتسبب لاحقا بهجمات نوع DoS			CVE-2011-4914
16	High	خطأ ذاكرة نوع heap-based buffer overflow في محلل الخطوط Parser AFM font قد يسمح للمهاجمين باطلاق هجمات نوع DoS او حتى بتنفيذ رمازات عشوائية انطلاقا من ملفات الخطوط	– DSA-2388 t1lib	٢٠١٢-١-١٤	CVE-2010-2642
17	Medium				CVE-2011-0433
18		ثغرة في برنامج Xpdf قبل3.02pl6 عبارة عن مؤشر غير صالح Invalid pointer dereference قد تسمح للمهاجمين بتنفيذ رمازات عشوائية بواسطة خط نوع type 1 في مستند PDF			CVE-2011-0764
19		ثغرة في برنامج Xpdf قبل3.02pl6 عبارة عن مؤشر غير صالح Invalid pointer dereference قد تسمح للمهاجمين بتنفيذ هجمات DoS نوع application crash بواسطة خط نوع type 1 في مستند PDF			CVE-2011-1552
20	Medium	ثغرة نوع Use-after-free في t1lib 5.1.2 والمستخدم في برامج قراءة ملفات pdf برنامج Xpdf قبل 3.02pl6 تسمح هذه الثغرة للمهاجمين باطلاق هجمات DoS نوع application crash بواسطة ملفات PDF			CVE-2011-1553
21	Medium	خطأ نوع Off-by-one في t1lib 5.1.2 والمستخدم في برامج قراءة ملفات pdf برنامج Xpdf قبل 3.02pl6 تسمح هذه الثغرة للمهاجمين باطلاق هجمات DoS نوع application crash بواسطة ملفات PDF	– DSA-2388 t1lib	٢٠١٢-١-١٤	CVE-2011-1554

Tel: +963 11 3937032 Fax: +963 11 3937079 E-mail: isc@nans.gov.sy Website: www.nans.gov.sy

22	High	عدة اخطاء نوع off-by-one في order_cmd.cpp في OpenTTD قبل ١,١,٣ تسمح هذه الاخطاء للمهاجمين باطلاق هجمات DoS نوع daemon crash وقد تسمح بتنفيذ رمازات خبيثة من خلال تعليمة CMD_INSERT_ORDER	DSA-2386-1 openttd	٢٠١٢-١-١٠	CVE-2011-3341
23		عدة مشاكل ذاكرة نوع buffer overflow في محاكي الالعاب OpenTTD قبل ١,١,٣ قد تسمح للمهاجمين باطلاق هجمات DoS نوع daemon crash وقد تسمح بتنفيذ رمازات خبيثة من خلال عدة متغيرات في الاجرائية Savegame			CVE-2011-3342
24		عدة مشاكل ذاكرة نوع buffer overflow في محاكي الالعاب OpenTTD قبل ١,١,٣ قد تسمح للمهاجمين باطلاق هجمات DoS نوع daemon crash او قد تسمح باكتساب بعض السماحيات			CVE-2011-3343
25	Unspecified	مخدم التحقق PowerDNS واستجابته للرزم المستقبلة، بحيث ان المهاجم اذا استطاع انتحال الIP المصدر للرزمة فانه يستطيع اطلاق هجمة DoS نوع endless packet loop بين PowerDNS و مخدم DNS	DSA-2385-1 pdns packet loop	٢٠١٢-١-١٠	CVE-2012-0206
26	Medium	ثغرة نوع XSS في CACTI قبل 0.8.7f قد تسمح للمهاجمين بحقن رمازات عشوائية من النوع HTML من خلال المتغيرات (1) hostname or (2) description وتمريرها الى الملف host.php	DSA-2384-1 cacti	٢٠١٢-١-9	CVE-2010-1644
27	Low	والمستخدم في حلول الحوسبة عالية المستوى HPC قد تسمح للمستخدمين البعيدين بسماحيات مدير نظام بتنفيذ تعليمات عشوائية بواسطة shell metacharacters			CVE-2010-1645
28	Medium	ثغرة نوع XSS في CACTI قبل 0.8.7f وتحديدا في الملف include/top_graph_header.php قد تسمح للمهاجمين بحقن رمازات			CVE-2010-2543

Tel: +963 11 3937032 Fax: +963 11 3937079 E-mail: isc@nans.gov.sy Website: www.nans.gov.sy

		عشوائية نوع HTML من خلال graph_start وتمريره للملف graph.php			
29	Low	ثغرة نوع XSS في CACTI قبل 0.8.7f قد تسمح للمهاجمين بحقن رمازات عشوائية من النوع HTML			CVE-2010-2545
30	Medium	ثغرة في CACTI قبل 0.8.7h نوع SQL injuction قد تسمح للمهاجمين بتنفيذ تعليمات SQL عشوائية من خلال البارامتر login_username			CVE-2011-4824
31	Medium	خطأ في التابع super.c في Super 3.30.0 يتسبب بخطأ نوع Buffer overflow مما قد يسمح للمستخدمين المحليين بتنفيذ رمازات خبيثة	DSA-2383-1 super-buffer overflow	٢٠١٢-١-٨	CVE-2011-2776
32	Unspecified	ثغرات ومشاكل في الأداة eCryptfs وهي احد انواع تشفير الملفات والمستخدمة في نظم التشغيل Linux	DSA-2382-1 ecryptfs-utils	٢٠١٢-١-٧	CVE-2011-1831 CVE-2011-1832 CVE-2011-1834 CVE-2011-1835 CVE-2011-1837 CVE-2011-3145
33	Medium	تابع idnsGrokReply في Squid قبل النسخة 3.1.16 لا يقوم بعمليات تحرير الذاكرة بالشكل الامثل ما يسمح للمهاجمين باطلاق هجمات DoS نوع daemon abort	DSA-2381-1 squid3	٢٠١٢-١-٦	CVE-2011-4096
34	Medium	اداة foomatic-rip-hplip في (HPLIP) 3.11.5	DSA-2380-1 foomatic-filters -- shell command injection	٢٠١٢-١-٤	CVE-2011-2697

Tel: +963 11 3937032 Fax: +963 11 3937079 E-mail: isc@nans.gov.sy Website: www.nans.gov.sy

35	Medium	Foomatic في foomaticrip.c 4.0.6 تسمح للمهاجمين بتنفيذ رمازات عشوائية بواسطة الحقل FoomaticRIPCommandLine في ملف .ppd	DSA-2380-1 foomatic-filters -- shell command injection	٢٠١٢-١-٤	CVE-2011-2964
36	High	ان تابع krb5_ldap_lockout_audit في خدمة التحقق MIT Kerberos 5 النسخ ١,٨,٤/١,٨/١,٩/١,٩,١ عندما تكون LDAP back end مستخدمة سيتمكن المهاجمون من تنفيذ هجمات DoS نوع assertion failure and daemon exit	DSA-2379-1 krb5	٢٠١٢-١-٤	CVE-2011-1528
37		ان تابع krb5_ldap_lockout_audit في خدمة التحقق MIT Kerberos 5 النسخ ١,٨,٤/١,٨/١,٩/١,٩,١ عندما تكون LDAP back end مستخدمة سيتمكن المهاجمون من تنفيذ هجمات DoS نوع NULL pointer dereference and daemon crash			CVE-2011-1529
38	Unspecified	عدة ثغرات مكتشفي في برنامج تشغيل ملفات الوسائط FFmpeg من حيث التراميز encoders للانواع: QDM2, VP5, VP6, VMD , SVQ1 قد تؤدي الى تنفيذ رمازات خبيثة	DSA-2378-1 ffmpeg	٢٠١٢-١-٣	CVE-2011-4351 CVE-2011-4353 CVE-2011-4364 CVE-2011-4579
39	Medium	خطأ في التابع index_get_ids في مخدم Cyrus IMAP قبل ٢,٤,١١ حيث تسمح للمهاجمين بتنفيذ هجمات DoS نوع NULL pointer dereference and daemon crash	DSA-2377-1 cyrus-imapd-2.2 -- NULL pointer dereference	٢٠١٢-١-١	CVE-2011-3481
40	Low	اداة ipmievd في OpenIPMI والمستخدمة في الحزمة ipmitool package 1.8.11 تسند السماحيات ٦٦٦ للملف ipmievd.pid PID file مما قد يسمح	DSA-2376-2 ipmitool -- insecure PID file	٢٠١١-١٢-٣٠	CVE-2011-4339

Tel: +963 11 3937032 Fax: +963 11 3937079 E-mail: isc@nans.gov.sy Website: www.nans.gov.sy

		للمستخدمين بعملية ايقاف الاجرائيات بواسطة الكتابة لهذا الملف			
41	High	خطأ نوع Buffer overflow في libtelnet/encrypt.c في التطبيق MIT Kerberos Version 5 النسخ ١,٠,٢ ١,٥,١ ومادون تسمح للمهاجمين بتنفيذ رمازات عشوائية بواسطة مفتاح تشفير طويل نسبيا	DSA-2375-1 krb5, krb5-appl -- buffer overflow	٢٠١١-١٢-٢٦	CVE-2011-4862

روابط التفاصيل الإضافية:

1. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4108
2. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4109
3. https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2011-4354
4. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4576
5. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4619
6. https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2011-2183
7. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-2213
8. https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2011-2898
9. https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2011-3353
10. https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2011-4077
11. https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2011-4110
12. https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2011-4127
13. https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2011-4611
14. https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2011-4622
15. https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2011-4914
16. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2642
17. https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2011-0433
18. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-0764
19. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-1552
20. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-1553
21. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-1554
22. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3341
23. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3342
24. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3343
25. http://www.debian.org/security/2012/dsa-2385
26. https://bugzilla.redhat.com/show_bug.cgi?id=609093
27. https://bugzilla.redhat.com/show_bug.cgi?id=609115
28. https://bugzilla.redhat.com/show_bug.cgi?id=541279
29. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2545
30. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-4824
31. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-2776
32. http://www.debian.org/security/2012/dsa-2382

Tel: +963 11 3937032 Fax: +963 11 3937079 E-mail: isc@nans.gov.sy Website: www.nans.gov.sy

33. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4096
34. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-2697
35. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-2964
36. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-1528
37. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-1529
38. http://www.debian.org/security/2012/dsa-2378
39. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3481
40. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4339
41. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4862
42. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0050
43. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-2930
44. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-2931
45. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3186
46. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-4214
47. http://www.debian.org/security/2012/dsa-2391
48. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3181
49. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4107

Tel: +963 11 3937032 Fax: +963 11 3937079 E-mail: isc@nans.gov.sy Website: www.nans.gov.sy

4. الثغرات الأمنية الموجودة في نظام التشغيل MAC OSX Server:

إسم الثغرة	التاريخ	نوع الثغرة	الوصـــــف	عامل الخطورة ٠ -- ١٠	تفاصيل إضافية مع حزم التحديث
CVE-2011-3463	2012-02-03	+Priv	WebDAV Sharing in Apple Mac OS X 10.7.x before 10.7.3 لا تقوم بعملية تحقق بالشكل الامثل مما قد يسمح للمستخدمين المحليين بربح سماحيات اضافية من خلال النفاذ الى المخدم	٧,٢	1
CVE-2011-3462		+Info	وقت المخدم في نظام Apple Mac OS X before 10.7.3 لا يقوم بعملية التحقق من المعرف الوحيد البعيد لـ AFP volume مما قد يسمح للمهاجمين بالحصول على معلومات حساسة والموجودة في النسخ الاحتياطية الجديدة	٥,٠	2
CVE-2011-3460		DoS Exec Code Overflow	خطا نوع Buffer overflow في التطبيق QuickTime in Apple Mac OS X before 10.7.3 تسمح للمهاجمين بتنفيذ رمازات عشوائية او اطلاق هجمات DoS نوع application crashبواسطة ملف نوع PNG	٧,٥	3
CVE-2011-3459			خطا نوع Off-by-one في مشغل الوسائط QuickTime in Apple Mac OS X before 10.7.3 تسمح للمهاجمين بتنفيذ رمازات عشوائية او اطلاق هجمات DoS نوع application crashبواسطة ملف movie	٦,٨	4
CVE-2011-3458		DoS Exec Code	QuickTime in Apple Mac OS X before 10.7.3 لا يمنع النفاذ الى مواقع غير مهيئة في الذاكرة مما يسمح للمهاجمين بتنفيذ رمازات عشوائية او التسبب بمنع تقديم الخدمة نوع application crash بواسطة ملف MP4		5
CVE-2011-3457		DoS Exec Code Overflow Mem. Corr.	تطبيق دعم الاظهار OpenGL في Apple Mac OS X before 10.7.3 لا تقوم بالترجمة الصحيحة للغة البرمجة OpenGL Shading Language مما يسمح للمهاجمين بتنفيذ رمازات عشوائية او التسبب بمنع تقديم الخدمة نوع memory corruption and application crash	٧,٥	6

Tel: +963 11 3937032 Fax: +963 11 3937079 E-mail: isc@nans.gov.sy Website: www.nans.gov.sy

7		خطا نوع Integer overflow في libresolv in Apple Mac OS X before 10.7.3 يسمح للمهاجمين بتنفيذ رمازت عشوائية او التسبب بمنع تقديم الخدمة نوع (heap memory corruption and application crash من خلال بيانات DNS			CVE-2011-3453
8	4.3	ان خدمة Internet Sharing في المخدم Apple Mac OS X before 10.7.3 لا تحافظ على اعدادات ال Wi-Fi اثناء التحديث مما يسمح للمهاجمين بالحصول على معلومات حساسة مستغلين ضعف/نقص كلمة مرور WEP في شبكات Wi-Fi	+Info	2012-02-03	CVE-2011-3452
9	٦,٨	ان الواجهة الرسومية CoreUI في النظام Apple Mac OS X 10.7.x before 10.7.3 لا تضع قيود على عمليات تخصيص مكدس الذاكرة مما يسمح للمهاجمين بتنفيذ رمازات عشوائية او التسبب بمنع تقديم الخدمة من النوع memory consumption and application crash	DoS Exec Code	2012-02-03	CVE-2011-3450
10	٦,٨	ثغرة نوع Use-after-free في التطبيق CoreText في النظام Apple Mac OS X before 10.7.3 تسمح للمهاجمين بتنفيذ رمازات خبيثة او منع تقديم الخدمة من النوع application crash من خلال نوع خط مدمج في مستند	DoS Exec Code	2012-02-03	CVE-2011-3449
11		خطا Heap-based buffer overflow في التطبيق CoreMedia في النظام Apple Mac OS X before 10.7.3 تسمح للمهاجمين بتنفيذ رمازات خبيثة او منع تقديم الخدمة من النوع application crash من خلال ملف فيلم بترميز H.264	DoS Exec Code Overflow		CVE-2011-3448
12	٤,٣	ان تطبيق CFNetwork في النظام Mac OS X 10.7.x before 10.7.3 لا تقوم بعملية بناء صحيحة للترويسة خلال تفسير طلبات URL مما يسمح للمهاجمين بالحصول على معلومات حساسة بواسطة طلبات URL غير قياسية	+Info		CVE-2011-3447
13	٧,٥	مجموعة خدمات Apple Type Services (ATS) في النظام Apple Mac OS X before 10.7.3 لا تقوم بادارة الذاكرة الخاصة بملفات data-font بالشكل الصحيح مما يسمح للمهاجمين بتنفيذ	DoS Exec Code	2012-02-03	CVE-2011-3446

Tel: +963 11 3937032 Fax: +963 11 3937079 E-mail: isc@nans.gov.sy Website: www.nans.gov.sy

		رمازات خبيثة او منع تقديم الخدمة من النوع application crash من خلال ملف خط			
14	٤,٣	سجل العناوين Address Book في النظام Apple Mac OS X before 10.7.3 يتحول بشكل ذاتي الى الجلسة غير المشفرة بعد فشل الجلسة المشفرة مما يسمح للمهاجمين بقراءة بيانات بطاقات CardDAV بعد ايقاف عمل التشفير والتجسس على الشبكة	--	2012-02-06	CVE-2011-3444
15	٦,٨	خطأ نوع Integer signedness في مجموعة الخدمات Apple Type Services (ATS) في نسخة النظام Mac OS X 10.7 قبل ١٠,٧,٢ يسمح للمهاجمين بتنفيذ رمازات عشوائية من خلال خطوط مضمنة نوع type1 في المستند	Exec Code	2012-01-13	CVE-2011-3437
16	٦,٥	خطأ دليل (مجلد) مفتوح في نسخة النظام Mac OS X 10.7 قبل 10.7.2 لا يجبر المستخدم على ادخال كلمة المرور الصحيحة قبل تغيير هذه الكلمة وهذا يسمح للمهاجمين بتجاوز قيود تغيير كلمة المرور	Bypass		CVE-2011-3436
17	٢,١	خطأ دليل (مجلد) مفتوح في نسخة النظام Mac OS X 10.7 قبل 10.7.2 يسمح للمستخدمين المحليين بقراءة بيانات كلمة المرور	--	2011-09-13	CVE-2011-3435
18	4.3	تطبيق تسلسل المفاتيح Keychain في نسخ النظام Mac OS 10.6.8 وما دون لا تقوم بالمعالجة الصحيحة للسمات غير الموثوقة لـ Certification Authority مما يسهل هجمات MITM بحيث يستطيع المهاجمون محاكاة مخدم SSL بواسطة النفاذ ب https من خلال Safari	--	2011-09-13	CVE-2011-3422
19	5.0	خدمة الشبكة CFNetwork في نظام Apple iOS قبل ٥,٠,١ وفي نسخة النظام Mac OS X 10.7 قبل 10.7.2 لا تقوم بالتحليل Parse الصحيح للروابط URLs مما يسمح للمهاجمين باطلاق طلبات لمواقع غير مقصودة اساسا من خلال روابط http/https	+Info	2012-01-13	CVE-2011-3246
20	٦,٨	مشغل الوسائط المتعددة QuickTime في النظام Apple Mac OS X before 10.7.2 يسمح للمهاجمين بتنفيذ رمازات عشوائية او التسبب بمنع تقديم الخدمة من النوع memory corruption and application crash بواسطة ملف فيلم	DoS Exec Code Mem. Corr.	2012-01-13	CVE-2011-3228

Tel: +963 11 3937032 Fax: +963 11 3937079 E-mail: isc@nans.gov.sy Website: www.nans.gov.sy

21		ان الـ libsecurity في النظام Apple Mac OS X before 10.7.2 لا يتعامل مع الخطاء بالشكل الامثل خلال عملية معالجة الامتدادات غير القياسية في Certificate Revocation list (CRL) مما يسمح للمهاجمين بتنفيذ رمازات عشوائية او التسبب بمنع تقديم الخدمة من النوع application crash من خلال e-mail message--web site	DoS Exec Code		CVE-2011-3227
22		خطأ من النوع Open Directory في النظام Apple Mac OS X 10.7 before 10.7.2 عند استخدام LDAPv3 server مع RFC 2307 يسمح للمهاجمين بتجاوز قيود طلب كلمة المرور من خلال استغلال فقدان سمة حساب المستخدم التالية AuthenticationAuthority	Bypass		CVE-2011-3226
23	5.0	ان مخدم SMB في النظام Apple Mac OS X 10.7 before 10.7.2 لا يمنع المستخدمين الـ guests من النفاذ الى share point record للمجلد guest-restricted مما يسمح للمهاجمين بتجاوز قيود التصفح من خلال الاستفادة من النفاذ بواسطة حساب nobody			CVE-2011-3225
24	٢,٦	ان User Documentation component في النظام Apple Mac OS X through 10.6.8 يستخدم جلسات اتصال من النوع http من اجل تحديثات App Store مما يسمح للمهاجمين ذوي اسلوب MITM بتنفيذ رمازات عشوائية	Exec Code		CVE-2011-3224
25	٦,٨	خطأ ذاكرة نوع Buffer overflow في مشغل الوسائط QuickTime في النظام Apple Mac OS X before 10.7.2 يسمح للمهاجمين بتنفيذ رمازات عشوائية او التسبب بمنع تقديم الخدمة نوع application crash من خلال ملف فيلم نوع FLIC	DoS Exec Code Overflow		CVE-2011-3223
26	٦,٨	خطأ ذاكرة نوع Buffer overflow في مشغل الوسائط QuickTime في النظام Apple Mac OS X before 10.7.2 يسمح للمهاجمين بتنفيذ رمازات عشوائية او التسبب بمنع تقديم الخدمة نوع application crash من خلال ملف FlashPix	DoS Exec Code Overflow	2012-01-13	CVE-2011-3222

Tel: +963 11 3937032 Fax: +963 11 3937079 E-mail: isc@nans.gov.sy Website: www.nans.gov.sy

27	٦,٨	ان مشغل الوسائط المتعددة QuickTime في Mac OS X before 10.7.2 لا يقوم بالتعامل الصحيح مع بنية التسلسل الهرمي في ملفات الافلام movie files مما يسمح للمهاجمين بتنفيذ رمازات عشوائية او التسبب بمنع تقديم الخدمة نوع application crash	DoS Exec Code	2012-01-13	CVE-2011-3221
28	٤,٣	ان مشغل الوسائط المتعددة QuickTime في Mac OS X before 10.7.2 لا يعالج بيانات الروابط URL بالشكل الامثل في ملفات الافلام مما يسمح للمهاجمين بالحصول على معلومات هامة من خلال مواقع في الذاكرة	Info+	2012-01-13	CVE-2011-3220
29	٢,٦	ان الامر Save for Web في مشغل الوسائط المتعددة QuickTime في Apple Mac OS X through 10.6.8 يقوم باستيراد مستندات HTML والتي قد تحوي روابط http تشير لملفات مما يسمح للمهاجمين بطريقة MITM باجراء عملية XSS من خلال التجسس على مخدم http اثناء عرض المستند المستورد	XSS	2012-01-13	CVE-2011-3218
30	٦,٨	ان مجموعة الادوات MediaKit في النظام Apple Mac OS X through 10.6.8 تسمح للمهاجمين بتنفيذ رمازات عشوائية او التسبب بمنع تقديم الخدمة نوع memory corruption and application crash من خلال ملف disk imag	DoS Exec Code Overflow Mem. Corr.		CVE-2011-3217
31	٢,١	ان النواة kernel في النظام Apple Mac OS X before 10.7.2 لا تقوم بتقديم الخانة sticky bit من أجل المجلدات مما قد يسمح للمستخدمين المحليين بتجاوز السماحيات وحذف بعض الملفات	Bypass		CVE-2011-3216
32		ان النواة kernel في النظام Apple Mac OS X before 10.7.2 لا تمنع النفاذ المباشر الى الذاكرة والخاص بوصلة FireWire بالشكل الامثل وذلك عند غياب الدخول login مما قد يسمح للمهاجمين القريبين بشكل كاف للاتصال الفيزيائي بتجاوز قيود الدخول واكتشاف كلمة المرور من خلال طلب DMA			CVE-2011-3215
33	٤,٦	ان الاظهار IOGraphics في النظام Apple Mac OS X through 10.6.8 لا يتعامل بالشكل الامثل مع الشاشة المؤمنة في حال سكون النظام وذلك للوضع			CVE-2011-3214

Tel: +963 11 3937032 Fax: +963 11 3937079 E-mail: isc@nans.gov.sy Website: www.nans.gov.sy

		Apple Cinema Display مما قد يسمح للمهاجمين القريبين بشكل كاف للاتصال الفيزيائي بتجاوز طلب كلمة المرور			
34	٧,٦	احد المكونات File Systems في النظام Apple Mac OS X before 10.7.2 لا يتتبع بالشكل الامثل شهادة X.509 والتي قد سبق وقبلها المستخدم بشكل يدوي وذلك لاتصال https WebDAV مما يسمح لمهاجمي MITM بخطف اتصال WebDAV	--	2012-01-13	CVE-2011-3213
35	٢,١	تطبيق CoreStorage في النظام Apple Mac OS X 10.7 before 10.7.2 لا يتحقق من كون جميع اقراص تخزين البيانات مشفرة اثناء عملية تفعيل FileVault مما يسهل على المهاجمين القريبين بشكل كاف للاتصال الفيزيائي الحصول على معلومات حساسة من خلال القراءة المباشرة من الاقراص	+Info	2012-01-13	CVE-2011-3212
36	٧,١	وظيفة الدعم GPU في النظام Mac OS X لا تقوم بالتقييد الامثل لوقت التقديم مما يسمح للمهاجمين بمنع تقديم الخدمة نوع desktop hang	DoS	٢٠١١-٠٧-١٢	CVE-2011-2601
37	٧,٦	في النظام Apple Mac OS X 10.5.x through 10.7.x لا تعمم القيود لجميع الاجراءات المنشأة مما يسمح للمهاجمين بالنفاذ الى موارد الشبكة	--	٢٠١٢-٠٢-١٦	CVE-2011-1516
38	٩,٣	خطا ذاكرة Integer overflow في التطبيق QuickLook والمستخدم في النظام Apple Mac OS X before 10.6.7 وفي التطبيق MobileSafari في النظام Apple iOS before 4.2.7 and 4.3.x before 4.3.2 يسمح للمهاجمين بتنفيذ رمازات عشوائية او التسبب بمنع تقديم الخدمة نوع memory corruption and application crash بواسطة مستند Microsoft Office	DoS Exec Code Overflow Mem. Corr.	2011-10-27	CVE-2011-1417
39	٤,٩	تطبيق IPv6 في النواة في النظام Apple Mac OS X before 10.6.8 يسمح للمستخدمين المحليين بالتسبب بمنع تقديم الخدمة نوع NULL pointer dereference and reboot بواسطة socket options	DoS	2011-10-26	CVE-2011-1132
40	٦,٩	ان النظام Apple Mac OS X لا يحذر المستخدم بالشكل الامثل اثناء تفعيل اجهزة نوع HID من خلال منافذ USB مما يسمح للمهاجمين	--	2011-04-28	CVE-2011-0639

Tel: +963 11 3937032 Fax: +963 11 3937079 E-mail: isc@nans.gov.sy Website: www.nans.gov.sy

		نوع user-assisted بتنفيذ رمازات عشوائية انطلاقا من اجهزة smartphone موصولة بطريقة ال USB			
41	٤,٣	ثغرة Stack consumption في التطبيق Apache Portable Runtime library before 1.4.3 and the Apache HTTP Server before 2.2.18 تسمح للمهاجمين بالتسبب بمنع تقديم الخدمة من النوع CPU and memory consumption	DoS	2012-01-18	CVE-2011-0419
42	٤,٦	ان مكون CoreProcesses في الظام Apple Mac OS X 10.7 before 10.7.2 لا تمنع نافذة النظام من استقبال ضغطات من لوحة المفاتيح في حال قفل الشاشة مما يسمح للمهاجمين القريبين بشكل كاف للاتصال الفيزيائي بتجاوز قيود النفاذ بواسطة الكتابة ضمن هذه النافذة	Bypass	2012-01-13	CVE-2011-0260
43	٥,٠	تطبيق CFNetwork في النظام Apple Mac OS X before 10.7.2 لا يقوم بالتتبع الامثل لخطة cookie-storage policy مما يسهل على مخدمات الويب البعيدة عملية تتبع المستخدمين بواسطة الcookie	+Info	2012-01-13	CVE-2011-0231
44	٧,٥	خطا ذاكرة نوع Buffer overflow في التطبيق ATSFontDeactivate API في الخدمات Apple Type Services (ATS) في النظام Apple Mac OS X before 10.7.2 يسمح للمهاجمين بتنفيذ رمازات عشوائية او التسبب بمنع تقديم الخدمة application crash	DoS Exec Code Overflow	2012-01-13	CVE-2011-0230
45	٦,٨	مجموعة الخدمات Apple Type Services (ATS) في النظام Apple Mac OS X through 10.6.8لا تتعامل بالشكل الامثل مع الخطوط المدمجة نوع Type 1 مما يسمح للمهاجمين بتنفيذ رمازات عشوائية بواسطة ملف مستند	Exec Code Overflow	2012-01-13	CVE-2011-0229
46	٦,٨	التطبيق CoreMedia في النظام Apple Mac OS X through 10.6.8 يسمح للمهاجمين بتنفيذ رمازات عشوائية او التسبب بمنع تقديم الخدمة نوع memory corruption بواسطة ملف نوع QuickTime movie	DoS Exec Code Mem. Corr.	2012-01-13	CVE-2011-0224
47	٦,٨	خطا ذاكرة نوع Buffer overflow في المشغل QuickTime في النظام Apple Mac OS X before 10.6.8 يسمح للمهاجمين بتنفيذ رمازات عشوائية او التسبب بمنع تقديم الخدمة نوع	DoS Exec Code Overflow	2011-08-10	CVE-2011-0213

Tel: +963 11 3937032 Fax: +963 11 3937079 E-mail: isc@nans.gov.sy Website: www.nans.gov.sy

		application crash بواسطة ملف نوع JPEG			
48		خطا ذاكرة نوع Integer overflow في المشغل QuickTime في النظام Apple Mac OS X before 10.6.8 يسمح للمهاجمين بتنفيذ رمازات عشوائية او التسبب بمنع تقديم الخدمة نوع application crash بواسطة ملف نوع movie			CVE-2011-0211
49	٦,٨	مشغل الوسائط المتعددة QuickTime في النظام Apple Mac OS X before 10.6.8 يسمح للمهاجمين بتنفيذ رمازات عشوائية او التسبب بمنع تقديم الخدمة نوع memory corruption and application crash بواسطة ملف نوع movie	DoS Exec Code Overflow Mem. Corr.	2011-10-26	CVE-2011-0210
50	٧,٥	خطا ذاكرة نوع Buffer overflow في التطبيق International Components for Unicode في النظام Apple Mac OS X before 10.6.8 application crash بواسطة محارف في الحالة uppercase	DoS Exec Code Overflow	2011-11-21	CVE-2011-0206
51		خطا من النوع Off-by-one في اطار العمل CoreFoundation framework في النظام Apple Mac OS X before 10.6.8 يسمح للمهاجمين بتنفيذ رمازات عشوائية او التسبب بمنع تقديم الخدمة نوع application crash بواسطة محرف CFString الذي يتسبب بدوره بـ buffer overflow		2011-07-22	CVE-2011-0201
52	٧,٨	الـ AirPort في النظام Apple Mac OS X 10.5.8 يسمح للمهاجمين بالتسبب بمنع تقديم الخدمة نوع out-of-bounds read and reboot بواسطة اطارات Wi-Fi في شبكة لاسلكية	DoS	2011-06-27	CVE-2011-0196

روابط التفاضيل الإضافية:

1. http://www.cvedetails.com/cve/CVE-2011-3463/
2. http://www.cvedetails.com/cve/CVE-2011-3462/
3. http://www.cvedetails.com/cve/CVE-2011-3460/
4. http://www.cvedetails.com/cve/CVE-2011-3459/
5. http://www.cvedetails.com/cve/CVE-2011-3458/
6. http://www.cvedetails.com/cve/CVE-2011-3457/
7. http://www.cvedetails.com/cve/CVE-2011-3453/
8. http://www.cvedetails.com/cve/CVE-2011-3452/
9. http://www.cvedetails.com/cve/CVE-2011-3450/
10. http://www.cvedetails.com/cve/CVE-2011-3449/
11. http://www.cvedetails.com/cve/CVE-2011-3448/

Tel: +963 11 3937032 Fax: +963 11 3937079 E-mail: isc@nans.gov.sy Website: www.nans.gov.sy

12. http://www.cvedetails.com/cve/CVE-2011-3447/
13. http://www.cvedetails.com/cve/CVE-2011-3446/
14. http://www.cvedetails.com/cve/CVE-2011-3444/
15. http://www.cvedetails.com/cve/CVE-2011-3437/
16. http://www.cvedetails.com/cve/CVE-2011-3436/
17. http://www.cvedetails.com/cve/CVE-2011-3435/
18. http://www.cvedetails.com/cve/CVE-2011-3422/
19. http://www.cvedetails.com/cve/CVE-2011-3246/
20. http://www.cvedetails.com/cve/CVE-2011-3228/
21. http://www.cvedetails.com/cve/CVE-2011-3227/
22. http://www.cvedetails.com/cve/CVE-2011-3226/
23. http://www.cvedetails.com/cve/CVE-2011-3225/
24. http://www.cvedetails.com/cve/CVE-2011-3224/
25. http://www.cvedetails.com/cve/CVE-2011-3223/
26. http://www.cvedetails.com/cve/CVE-2011-3222/
27. http://www.cvedetails.com/cve/CVE-2011-3221/
28. http://www.cvedetails.com/cve/CVE-2011-3220/
29. http://www.cvedetails.com/cve/CVE-2011-3218/
30. http://www.cvedetails.com/cve/CVE-2011-3217/
31. http://www.cvedetails.com/cve/CVE-2011-3216/
32. http://www.cvedetails.com/cve/CVE-2011-3215/
33. http://www.cvedetails.com/cve/CVE-2011-3214/
34. http://www.cvedetails.com/cve/CVE-2011-3213/
35. http://www.cvedetails.com/cve/CVE-2011-3212/
36. http://www.cvedetails.com/cve/CVE-2011-2601/
37. http://www.cvedetails.com/cve/CVE-2011-1516/
38. http://www.cvedetails.com/cve/CVE-2011-1417/
39. http://www.cvedetails.com/cve/CVE-2011-1132/
40. http://www.cvedetails.com/cve/CVE-2011-0639/
41. http://www.cvedetails.com/cve/CVE-2011-0419/
42. http://www.cvedetails.com/cve/CVE-2011-0260/
43. http://www.cvedetails.com/cve/CVE-2011-0231/
44. http://www.cvedetails.com/cve/CVE-2011-0230/
45. http://www.cvedetails.com/cve/CVE-2011-0229/
46. http://www.cvedetails.com/cve/CVE-2011-0224/
47. http://www.cvedetails.com/cve/CVE-2011-0213/
48. http://www.cvedetails.com/cve/CVE-2011-0211/
49. http://www.cvedetails.com/cve/CVE-2011-0210/
50. http://www.cvedetails.com/cve/CVE-2011-0206/
51. http://www.cvedetails.com/cve/CVE-2011-0201/
52. http://www.cvedetails.com/cve/CVE-2011-0196/

Tel: +963 11 3937032 Fax: +963 11 3937079 E-mail: isc@nans.gov.sy Website: www.nans.gov.sy

5. الثغرات الأمنية الموجودة في نظام التشغيل SUSE Linux Enterprise Server:

إسم الثغرة	التاريخ	نوع الثغرة	الوصـــــف	عامل الخطورة ١٠ -- ٠	تفاصيل إضافية مع حزم التحديث
CVE-2010-0230	2011-04-28	Bypass	ان اصدار النظام SUSE Linux Enterprise 10 SP3 (SLE10-SP3) ، openSUSE 11.2 تقوم باعداد الـ postfix بحيث يقوم بالتنصت على جميع واجهات الشبكة مما قد يسمح للمهاجمين بتجاوز القيود الالزامية للوصول الى النظام	٧,٥ High	1
CVE-2011-3171	٢٠١١-١١-٧	Directory Traversal	ثغرة (تجاوز المجلد) في الاداة pure-FTPd 1.0.22 وعلى الارجح الاصدارات الاخرى ، عندما تكون الاداة Netware OES remote server في وضعية التفعيل قد تسمح للمستخدمين المحليين باعادة نسخ بعض الملفات overwrite	٣,٦ Low	2
CVE-2011-2660	٢٠١١-١٠-٢٦	Exec Code	modify_resolvconf_suse script في الحزمة vpnc package before 0.5.1-55.10.1 قد تسمح للمهاجمين بتنفيذ تعليمات عشوائية بواسطة اسم DNS domain	٧,٥ High	3
CVE-2011-0995	٢٠١١-٥-٢٦	+Priv	ان الاداة sqlite3-ruby في الحزمة rubygem-sqlite3 before 1.2.4-0.5.1 تعتمد على قيود سماحيات ضعيفة لبعض الملفات مما قد يسمح للمستخدمين المحليين بربح بعض السماحيات الاضافية	٢,١ Low	4
CVE-2011-0988	٢٠١١-٤-١٨		ان الاداة pure-ftpd 1.0.22 عند تشغيل OES Netware تقوم بانشاء مجلد مع خاصية الكتابة مما يسمح للمستخدمين المحليين باستبدال بعض الملفات وربح سماحيات اضافية	٤,٤ Medium	5
CVE-2010-3912	٢٠١١-١-٢٢	--	ان رماز supportconfig في supportutils لا يقوم بعملية (تمويه) مناسبة لكلمة السر في ملفات الاعدادات مما قد يسمح بكشف كلمة السر	١٠,٠ High	6
CVE-2010-3110	٢٠١٠-١٠-١٣	Overflow +Priv	عدة اخطاء ذاكرة في Novell Client novfs module for the Linux kernel قد تسمح هذه الاخطاء للمستخدمين المحليين بربح سماحيات اضافية	٧,٢ High	7

Tel: +963 11 3937032 Fax: +963 11 3937079 E-mail: isc@nans.gov.sy Website: www.nans.gov.sy

8	٥,٠ Medium	ان الاداة WebYaST في yast2-webclient تقوم باستخدام مفتاح سري ثابت وهو مدمج في WebYaST appliance مما قد يسمح للمهاجمين بانتحال الجلسة الحالية من خلال استغلال معرفة هذا المفتاح	+Info	٢٠١٠-٩-٦	CVE-2010-1507
9	٤,٣ Medium	ثغرة في الحزمة apache2-slms تسمح للمهاجمين باختطاف بيانات المصادقة من خلال بعض عمليات اقتباس البارمترات	XSS	٢٠١٠-٩-٦	CVE-2010-1325
10	٦,٢ Medium	ان gdk/gdkwindow.c in GTK+ before 2.18.5 والمستخدمة في gnome-screensaver before 2.28.1 تستخدم الوانا مضمنة في النوافذ نوع GDK_WINDOW_FOREIGN مما قد يولد خطأ نوع X error في ظروف خاصة مما قد يسمح للمهاجمين القريبين فيزيائيا بتجاوز قفل الشاشة والنفاذ الى نظام الطرفية من خلال تكرار الضغط على المفتاح ENTER	+Bypass	٢٠١٠-٦-٥	CVE-2010-0732
11	٤,٤ Medium	iscsi_discovery in open-iscsi تسمح للمستخدمين المحليين باستبدال بعض الملفات بواسطة هجوم نوع symlink attack على ملف مؤقت قد يملك اسما قابلا للتنبؤ	--	٢٠٠٩-١٠-٢٩	CVE-2009-1297
12	٤,٩ Medium	ثغرة في الاداة ia32el before 7042_7022-0.4.2 قد تسمح للمستخدمين المحليين بالتسبب بمنع الخدمة نوع system crash	DoS	٢٠٠٩-٩-١٨	CVE-2009-2707
13	٧,٥ High	ان البرتوكول YaST2 LDAP في yast2-ldap-server لا يقوم بعملية التفعيل اللازمة للجدار الناري في ظروف معينة (اعادة الاقلاع اثناء التحديثات) مما يسمح للمهاجمين بالنفاذ الى خدمات الشبكة	--	٢٠٠٩-٧-٦	CVE-2009-1648
14	٤,٣ Medium	ثغرة في Apache Struts before 1.2.9-162.31.1 قد تسمح للمهاجمين بحقن رمازات نوع web script/HTML من خلال عمليات insufficient quoting of parameters	XSS	٢٠٠٩-٤-١٨	CVE-2008-2025
15	٧,٢ High	aka multipath-tools or device-mapper-multipath) 0.4.8 تستخدم سماحيات نوع world-writable من اجل الملف aka /var/run/multipathd.sock مما قد يسمح للمستخدمين المحليين بتنفيذ تعليمات عشوائية	Exec Code	٢٠١٠-٨-٢١	CVE-2009-0115

Tel: +963 11 3937032 Fax: +963 11 3937079 E-mail: isc@nans.gov.sy Website: www.nans.gov.sy

CVE-2006-5616	2011-09-02	Exec Code	عدة ثغرات في الاداة OpenPBS في النظام SUSE Linux 9.2 through 10.1 قد تسمح للمهاجمين بتنفيذ رمازات خبيثة	١٠,٠ High	16
CVE-2007-0460	2010-09-15	Overflow	عدة اخطاء ذاكرة نوع buffer overflow في SUSE Linux 9.3 up to 10.1 تتعلق بمشاكل التعامل غير الصحيح باحتساب اطوال السلاسل المحرفية improper string length calculations	١٠,٠ High	17
CVE-2005-3625	2010-10-18	DoS	ان برنامج قراءة ملفات Xpdf والمستخدم ضمن البرامج gpdf, kpdf, pdftohtml, poppler, teTeX, CUPS, libextractor تسمح للمهاجمين بالتسبب بمنع تقديم الخدمة من النوع infinite loop اثناء التدفقات غير المكتملة والتي قد تتظاهر كالتدفقات: CTDecode streams CCITTFaxDecode	١٠,٠ High	18
CVE-2005-0605	2010-08-21	Exec Code Overflow	الاجرائية scan.c في LibXPM تسمح للمهاجمين بتنفيذ رمازات خبيثة بواسطة قيمة سلبية للباراميتر bitmap_unit والتي تؤدي بدورها الى خطأ buffer overflow	٧,٥ High	19
CVE-2004-1154	2010-08-21	DoS Exec Code Overflow	خطا ذاكرة نوع Integer overflow في البرنامج Samba 2.x and 3.0.x through 3.0.9 قد تسمح للمستخدمين البعيدين بالتسبب بمنع تقديم الخدمة من النوع application crash واحتمال تنفيذ رمازات عشوائية	١٠,٠ High	20

روابط التفاضيل الإضافية:

1. http://www.cvedetails.com/cve/CVE-2010-0230/
2. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3171
3. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-2660
4. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-0995
5. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-0988
6. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-3912
7. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-3110
8. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-1507
9. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-1325
10. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0732
11. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-1297
12. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-2707
13. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-1648
14. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-2025

Tel: +963 11 3937032 Fax: +963 11 3937079 E-mail: isc@nans.gov.sy Website: www.nans.gov.sy

15. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-0115
16. http://www.cvedetails.com/cve/CVE-2006-5616/
17. http://www.cvedetails.com/cve/CVE-2007-0460/
18. http://www.cvedetails.com/cve/CVE-2005-3625/
19. http://www.cvedetails.com/cve/CVE-2005-0605/
20. http://www.cvedetails.com/cve/CVE-2004-1154/

Tel: +963 11 3937032 Fax: +963 11 3937079 E-mail: isc@nans.gov.sy Website: www.nans.gov.sy

6. المراجـــــع:

Http://www.ubuntu.com
http://www.cve.mitre.org
http://nvd.nist.gov
http://www.kb.cert.org/
http://www.redhat.com
https://bugzilla.redhat.com/
http://www.cvedetails.com
http://www.itsecdb.com
http://www.technet.microsoft.com
http://www.microsoft.com/
http://www.debian.org
http://www.exploit-db.com
http://www.suse.com

Tel: +963 11 3937032 Fax: +963 11 3937079 E-mail: isc@nans.gov.sy Website: www.nans.gov.sy