جدول آخرین به‌روزرسانی‌ها و آسیب‌پذیری‌های نرم‌افزارهای پرکاربرد در کشور

سرویس‌دهنده‌ها (وب، پست الکترونیک، پراکسی و غیره)

دریافت آخرین نسخه‌ی پایدار

موضوع	آخرین نسخه‌ی پایدار	تاریخ عرضه	لینک دریافت
Apache Web Server	2.4.20	2015-04-11	goo.gl/ySdR
Squid Proxy & Cache Server	3.5.17	2016-04-20	goo.gl/ZCyZ6f

آسیب‌پذیری‌ها

موضوع	شناسه	منبع	تاریخ انتشار	سطح خطر	خلاصه‌ای از آسیب‌پذیری	نحوه رفع	اطلاعات بیشتر
Samba	CVE-2016-2118	goo.gl/mGZMhl	2016-04-13	متوسط	آسیب‌پذیری‌های افزایش سطح دسترسی و جعل کاربر در Samba توسط مهاجمین MitM به علت وجود نقص در پیاده‌سازی پروتکل‌های MS-SAMR و MS-LSAD	آسیب‌پذیری‌های فوق در Samba نسخه‌های 4.2.11، 4.3.8 و 4.4.2 برطرف گردیده است. goo.gl/JxwcMs	goo.gl/RBkahD
dhcpcd	CVE-2012-6700 CVE-2012-6699 CVE-2012-6698	goo.gl/XXUvA1 goo.gl/tYU8eF goo.gl/iMqO2X	2016-04-13	زیاد	چندین آسیب‌پذیری جلوگیری از سرویس در dhcpcd نسخه‌های 3.x به واسطه‌ی وجود نقص در تابع decode_search با استفاده از یک پاسخ جعلی	آسیب‌پذیری‌های فوق در Debian برطرف گردیده است. goo.gl/srrpbS	goo.gl/XIFHk6 goo.gl/EKXMA8 goo.gl/OpsMEz
Squid	CVE-2016-3948 CVE-2016-3947	goo.gl/aFDK0x goo.gl/vlrxay	2016-04-02	زیاد	آسیب‌پذیری‌های جلوگیری از سرویس و آشکارسازی اطلاعات حساس در سرویس‌دهنده‌ی Squid با استفاده از یک پاسخ HTTP جعلی و یا یک بسته‌ی ICMPv6 جعلی	آسیب‌پذیری‌های فوق در سرویس‌دهنده‌ی Squid نسخه‌های 3.5.16 و 4.0.8 برطرف گردیده است. goo.gl/ZCyZ6f	goo.gl/UHF7hJ goo.gl/Gt48W0

موضوع	شناسه	منبع	تاریخ انتشار	سطح خطر	خلاصه‌ای از آسیب‌پذیری	نحوه رفع	اطلاعات بیشتر
Samba	CVE-2016-0771 CVE-2015-7560	goo.gl/FfCcLW goo.gl/cKlnHK	2016-03-13	----	آسیب‌پذیری‌های جلوگیری از سرویس، به دست آوردن اطلاعات حساس و همچنین ایجاد تغییر در فهرست کنترل دسترسی در Samba به علت وجود نقص در سرویس‌دهنده‌ی DNS داخلی و پیاده‌سازی SMB1	آسیب‌پذیری‌های فوق در Samba نسخه‌های 4.1.23، 4.2.9، 4.3.6 و 4.4.0rc4 برطرف گردیده‌اند. goo.gl/JxwcMs وصله برای نسخه‌های 4.3.5، 4.2.8 و 4.1.22 : goo.gl/wDWhb4	goo.gl/rcIhWX goo.gl/Fe4yFL
BIND	CVE-2016-2088 CVE-2016-1286 CVE-2016-1285	goo.gl/RmYI7z goo.gl/Ge4mN6 goo.gl/yatSdg	2016-03-09	زیاد	چندین آسیب‌پذیری جلوگیری از سرویس در ISC BIND نسخه‌های ماقبل 9.10.3-P4 و 9.9.8-P4	آسیب‌پذیری‌های فوق در ISC BIND نسخه‌های 9.10.3-P4 و 9.9.8-P4 برطرف گردیده است. goo.gl/KQtfv0	goo.gl/78UZYI goo.gl/O18imC goo.gl/rL5XLm
DHCP	CVE-2016-2774	goo.gl/r6DNPa	2016-03-07	متوسط	آسیب‌پذیری جلوگیری از سرویس در ISC DHCP به واسطه‌ی عدم اعمال محدودیت مؤثر روی نشست‌های TCP همزمان	آسیب‌پذیری فوق در ISC DHCP نسخه‌های 4.1-ESV-R13 و 4.3.4 برطرف گردیده است. goo.gl/KQtfv0	goo.gl/FJD0XC

سیستم‌های عامل

موضوع	شناسه	منبع	تاریخ انتشار	سطح خطر	خلاصه‌ای از آسیب‌پذیری	نحوه رفع	اطلاعات بیشتر
Windows	MS16-050	goo.gl/IgFWHQ	2016-04-12	زیاد	چندین آسیب‌پذیری دور زدن محدودیت‌های امنیتی، اجرای کد دلخواه، افزایش سطح دسترسی، خرابی حافظه و جلوگیری از سرویس در ویندوز به واسطه‌ی وجود نقص در Adobe Flash Player	برای ویندوز 8.1 32bit : goo.gl/QiADhn برای ویندوز 8.1 64bit : goo.gl/TRCrCG برای ویندوز Server 2012 R2 : goo.gl/Mv4PMj	goo.gl/IgFWHQ
Windows	MS16-049	goo.gl/Szt9kN	2016-04-12	متوسط	آسیب‌پذیری جلوگیری از سرویس در ویندوز 10 نسخه‌های Gold و 1511 به واسطه‌ی وجود نقص در HTTP.sys با استفاده از ارسال یک بسته‌ی HTTP جعلی به سیستم قربانی	ویندوز 10 را به‌روزرسانی نمائید. KB3147461 KB3147458	goo.gl/hXTSII

Windows	MS16-048	goo.gl/WqDTbP	2016-04-12	متوسط	آسیب‌پذیری دور زدن محدودیت‌های امنیتی در ویندوز به واسطه‌ی وجود نقص در CSRSS در صورت ورود مهاجم به سیستم قربانی و اجرای یک برنامه‌ی کاربردی مخرب	برای ویندوز 8.1 64bit : goo.gl/XGsUCP برای ویندوز Server 2012 R2 : goo.gl/wjpLh1 ویندوز 10 را به‌روزرسانی نمائید. KB3147461 KB3147458	goo.gl/ki3cNy
Windows	MS16-047	goo.gl/fjtt0W	2016-04-12	متوسط	آسیب‌پذیری افزایش سطح دسترسی در ویندوز با استفاده از حمله‌ی MitM و پایین آوردن سطح احراز هویت کانال‌های SAM و LSAD و در نهایت جعل هویت کاربر احراز هویت شده	برای ویندوز 7 SP1 64bit : goo.gl/LtxONn برای ویندوز 8.1 64bit : goo.gl/C8aBOc ویندوز 10 را به‌روزرسانی نمائید. KB3147461 KB3147458	goo.gl/SPH6WX
Windows	MS16-046	goo.gl/WFgFAS	2016-04-12	متوسط	آسیب‌پذیری اجرای کد دلخواه در سطح مدیر سیستم در نسخه‌های مختلف ویندوز 10 به واسطه‌ی وجود نقص در رسیدگی به درخواست‌ها در حافظه توسط Secondary Logon Service	ویندوز 10 را به‌روزرسانی نمائید. KB3147461 KB3147458	goo.gl/rQdFH1
Windows	MS16-044	goo.gl/5ysO2W	2016-04-12	متوسط	آسیب‌پذیری اجرای کد از راه دور در ویندوز به واسطه‌ی عدم بررسی مناسب ورودی کاربر توسط Windows OLE در صورت متقاعد شدن کاربر به باز کردن یک فایل یا برنامه‌ی جعلی	برای ویندوز 7 SP1 32bit : goo.gl/PEbg0C برای ویندوز 8.1 32bit : goo.gl/zKPUUc برای ویندوز Server 2012 R2 : goo.gl/ymAzJb	goo.gl/qriqU4
Windows	MS16-040	goo.gl/WUcRxF	2016-04-12	زیاد	آسیب‌پذیری اجرای کد از راه دور و به دست گرفتن کنترل سیستم در ویندوز به واسطه‌ی وجود نقص در MSXML 3.0 با متقاعد شدن قربانی برای کلیک کردن روی یک لینک جعلی	برای ویندوز 7 SP1 64bit : goo.gl/QybjLQ برای ویندوز 8.1 64bit : goo.gl/Xqudnk ویندوز 10 را به‌روزرسانی نمائید. KB3147461 KB3147458	goo.gl/SBVx4e

Windows	MS16-039	goo.gl/rDJs1j	2016-04-12	زیاد	چندین آسیب‌پذیری اجرای کد از راه دور در ویندوز، .NET Framework، Office، Skype for Business و Lync در صورت باز کردن یک سند جعلی و یا مشاهده‌ی یک صفحه‌ی وب شامل فونت‌های جعلی	برای ویندوز 7 SP1 32bit : goo.gl/o8K2Go برای ویندوز 8.1 32bit : goo.gl/j9zxOW ویندوز 10 را به‌روزرسانی نمائید. KB3147461 KB3147458	goo.gl/rDJs1j
FreeBSD	CVE-2016-1885	goo.gl/cw7DMK	2016-03-16	زیاد	آسیب‌پذیری جلوگیری از سرویس در سیستم عامل ۶۴ بیتی FreeBSD به واسطه‌ی وجود سرریزی بافر مبتنی بر هیپ هنگام فراخوانی i386_set_ldt	آسیب‌پذیری فوق در FreeBSD نسخه‌های 9.3 p39، 10.1 p31 و 10.2 p14 برطرف گردیده است.	goo.gl/f1lMPy
Apple iOS, OS X, tvOS, watchOS, Safari	CVE-2016-1788 CVE-2016-1787 CVE-2016-1786 , …	goo.gl/yt9qt9 goo.gl/Ew8J4K goo.gl/IGJzXl , …	2016-03-21	متوسط	چندین آسیب‌پذیری شکستن سازوکار رمزنگاری، دور زدن سیاست‌های امنیتی، به دست آوردن اطلاعات حساس، اجرای کد دلخواه از راه دور و جلوگیری از سرویس در محصولات Apple	این آسیب‌پذیری‌ها در Apple iOS نسخه‌ی 9.3، Apple OS X نسخه‌ی 10.11.4، Apple tvOS نسخه‌ی 9.2، Apple watchOS نسخه‌ی 2.2 و Apple Safari نسخه‌ی 9.1 برطرف گردیده است.	goo.gl/w4fTfz goo.gl/D55K72 goo.gl/adXz7e , …
Debian Jessie	CVE-2016-2856	goo.gl/lKLHKJ	2016-03-13	متوسط	آسیب‌پذیری جعل داده‌ها و به افزایش سطح دسترسی در Debian Jessie به واسطه‌ی وجود نقص در glibc	آسیب‌پذیری فوق در صورت استفاده از glibc نسخه‌ی 2.19-18+deb8u4 روی Debian Jessie رفع می‌گردد.	goo.gl/Rw3DpC

محیط‌های برنامه‌نویسی

دریافت آخرین نسخه‌ی پایدار

موضوع	آخرین نسخه پایدار	تاریخ عرضه	لینک دریافت
Joomla!	**3.5.1**	**2016-04-05**	**goo.gl/ZEG0Nh**
Drupal	**8.1.0**	**2016-04-20**	**goo.gl/c5F8At**

WordPress	**4.5**	**2016-04-12**	**goo.gl/DK0Wx**
DotNetNuke	**8.00.02**	**2016-04-18**	**goo.gl/pT76iH**

آسیب‌پذیری‌ها

موضوع	شناسه	منبع	تاریخ انتشار	سطح خطر	خلاصه‌ای از آسیب‌پذیری	نحوه رفع	اطلاعات بیشتر
Cacti	CVE-2016-2313 CVE-2016-3172 CVE-2015-8604 CVE-2016-3659	goo.gl/H0R07D goo.gl/45MQ2x goo.gl/84mM0b goo.gl/gLRKbu	2016-04-13	زیاد	چندین آسیب‌پذیری تزریق SQL و دور زدن محدودیت‌های امنیتی در Cacti به واسطه‌ی وجود نقص در auth_login.php، tree.php، graph_view.php و graphs_new.php	آسیب‌پذیری با شناسه‌ی CVE-2016-2313 در Cacti نسخه‌ی 0.8.8g برطرف گردیده است. تاکنون راه حلی برای آسیب‌پذیری‌های تزریق SQL ارائه نگردیده است. goo.gl/DfSSDE	goo.gl/jLGcYK goo.gl/25fdmZ goo.gl/2hQzlG goo.gl/9HspD7
.NET Framework	MS16-041	goo.gl/Po7wZi	2016-04-12	متوسط	آسیب‌پذیری اجرای کد از راه دور در .NET Framework در صورت دسترسی مهاجم به سیستم قربانی و اجرای یک برنامه‌ی کاربردی مخرب	برای .NET Framework نسخه‌های 4.6 و 4.6.1 روی سیستم‌های عامل ویندوز Vista، Server 2008 R2 (GUI & Core Installation) و 7 : goo.gl/6Xu6zK	goo.gl/hdaHjp
Perl	CVE-2016-2381	goo.gl/M947xq	2016-04-08	----	آسیب‌پذیری دور زدن سازوکار امنیتی taint در Perl با استفاده از متغیرهای محیطی تکراری در envp	آسیب‌پذیری فوق در Debian برطرف گردیده است. goo.gl/gXCbNh	goo.gl/iCQukz
Drupal	VE-2016-3171 VE-2016-3170 VE-2016-3169 , …	goo.gl/rf77yp	2016-02-24	زیاد	چندین آسیب‌پذیری اجرای کد دلخواه، افزایش سطح دسترسی، سرقت احراز هویت، Phishing، تزریق CRLF، Brute-force و غیره در Drupal	آسیب‌پذیری‌های فوق در Drupal نسخه‌های 6.38، 7.43 و 8.04 برطرف گردیده است. goo.gl/c5F8At	goo.gl/rf77yp

Java SE	CVE-2016-0636	goo.gl/yauxcU	2016-03-23	----	آسیب‌پذیری‌های نامشخص پس از دور زدن سازوکار احراز هویت در Java SE نسخه‌های 7u97، 8u73 و 8u74 در صورت مشاهده‌ی یک صفحه‌ی وب مخرب توسط کاربر	برای رفع آسیب‌پذیری فوق، وصله‌های منتشر شده را نصب کنید و یا از آخرین نسخه‌ی Java SE استفاده نمائید. goo.gl/sVy6aP goo.gl/JFNnjz	goo.gl/mrHEKl
.NET Framework	MS16-035	goo.gl/ULXI6Y	2016-03-08	متوسط	آسیب‌پذیری دور زدن ویژگی امنیتی و جعل امضاء در .NET Framework. به واسطه‌ی عدم بررسی مناسب یک عنصر سند XML امضاء شده	برای .NET Framework 4.5.2 روی سیستم‌های عامل ویندوز 8.1، RT 8.1 و Server 2012 R2 : goo.gl/7eLR9G ویندوز 10 را به‌روزرسانی نمائید. KB3140745 KB3140768	goo.gl/etRs1L
GTK+	CVE-2013-7447	goo.gl/7bh29j	2016-02-17	----	آسیب‌پذیری جلوگیری از سرویس در GTK+ نسخه‌های ماقبل 3.9.8 به واسطه‌ی سرریزی مقدار عدد صحیح هنگام تخصیص حافظه‌ی زیاد در صورت استفاده از یک فایل عکس با حجم بالا	این آسیب‌پذیری در Ubuntu برطرف گردیده است. goo.gl/VNAZLh	goo.gl/R7eEAF
Python	CVE-2016-1494	goo.gl/gPYnV6	2016-01-15	متوسط	آسیب‌پذیری جعل امضا در در Python نسخه‌های ماقبل 3.3 به علت نقص در تابع verify در بسته‌ی RSA	این آسیب‌پذیری در Python نسخه‌ی 3.3 برطرف گردیده است. goo.gl/zD9zUP	goo.gl/zPlq3N

مرورگرهای اینترنت

دریافت آخرین نسخه‌ی پایدار

موضوع	آخرین نسخه پایدار	تاریخ عرضه	لینک دریافت
Mozilla Firefox	**45.0.2**	**2016-04-11**	**goo.gl/yIXtW**
Google Chrome	**50.0.2661.87**	**2016-04-20**	**goo.gl/Jk2diZ**

آسیب‌پذیری‌ها

موضوع	شناسه	منبع	تاریخ انتشار	سطح خطر	خلاصه‌ای از آسیب‌پذیری	نحوه رفع	اطلاعات بیشتر
Microsoft Edge	MS16-038	goo.gl/mhnVUf	2016-04-12	زیاد	چندین آسیب‌پذیری اجرای کد از راه دور و افزایش سطح دسترسی در مرورگر Microsoft Edge در صورت مشاهده‌ی یک صفحه‌ی وب جعلی	ویندوز 10 را به‌روزرسانی نمائید. KB3147461 KB3147458	goo.gl/mhnVUf
Internet Explorer	MS16-037	goo.gl/cch75d	2016-04-12	زیاد	چندین آسیب‌پذیری اجرای کد از راه دور، افزایش سطح دسترسی و ایجاد تغییرات در فایل‌ها در Internet Explorer در صورت مشاهده‌ی یک صفحه‌ی وب جعلی	برای مرورگر Internet Explorer نسخه‌ی 11 روی : ویندوز 7 SP1 32bit : goo.gl/ZI90pL ویندوز 7 SP1 64bit : goo.gl/TFW87Q ویندوز Server 2012 R2 : goo.gl/O5Kx5p ویندوز 10 را به‌روزرسانی نمائید. KB3147461 KB3147458	goo.gl/MTLb2d goo.gl/2Xdfuw
Google Chrome	CVE-2016-3679 CVE-2016-1650 CVE-2016-1649	goo.gl/KZPwnc goo.gl/52IZZn goo.gl/7lFQ8E , …	2016-03-29	زیاد	چندین آسیب‌پذیری سرریزی بافر و جلوگیری از سرویس در مرورگر Google Chrome نسخه‌های ماقبل 49.0.2623.108	آسیب‌پذیری‌های فوق در مرورگر Google Chrome نسخه‌ی 49.0.2623.108 برطرف گردیده است. goo.gl/Jk2diZ	goo.gl/rhJeVB goo.gl/UQEeV7 goo.gl/oiwNhr , …
Microsoft Edge	MS16-024	goo.gl/vcauGs	2016-03-08	زیاد	آسیب‌پذیری اجرای کد از راه دور و افزایش سطح دسترسی در مرورگر Microsoft Edge در صورت مشاهده‌ی یک صفحه‌ی وب جعلی	ویندوز 10 را به‌روزرسانی نمائید. KB3140745 KB3140768	goo.gl/vcauGs

Mozilla Firefox	CVE-2016-2802 CVE-2016-2801 CVE-2016-2800 , …	goo.gl/8sY1jx goo.gl/GevFH7 goo.gl/BT8ypa , …	2016-03-08	زیاد	چندین آسیب‌پذیری خرابی حافظه، سرریزی بافر، دور زدن محدودیت‌های امنیتی، به دست آوردن اطلاعات حساس، جلوگیری از سرویس و غیره در مرورگر Mozilla Firefox	آسیب‌پذیری‌های فوق در مرورگر Mozilla Firefox نسخه‌ی 45.0 برطرف گردیده است. goo.gl/yIXtW	goo.gl/0IHQ1D goo.gl/DNzxmt goo.gl/zxPEk6 , …

مجازی‌سازی

دریافت آخرین نسخه‌ی پایدار

موضوع	آخرین نسخه پایدار	تاریخ عرضه	لینک دریافت
VirtualBox	**5.0.18**	**2016-04-18**	**goo.gl/l3wrf**

آسیب‌پذیری‌ها

موضوع	شناسه	منبع	تاریخ انتشار	سطح خطر	خلاصه‌ای از آسیب‌پذیری	نحوه رفع	اطلاعات بیشتر
VMware	CVE-2016-2076	goo.gl/qzxwhh	2016-04-14	----	آسیب‌پذیری ربودن نشست در VMware vCenter Server، vCloud Director و vRA Identity Appliance به واسطه‌ی وجود نقص در CIP با استفاده از یک وب‌سایت جعلی	آسیب‌پذیری فوق در vCenter Server نسخه‌ی 6.0 U2 و 5.5 U3d، در vCloud Director نسخه‌ی 5.5.6 در ویندوز و در vRA Identity Appliance نسخه‌ی 6.2.4.1 در لینوکس برطرف گردیده است. پس از اعمال به‌روزرسانی‌های فوق، می‌بایست CIP نیز به‌روزرسانی گردد. goo.gl/TnkS6W goo.gl/ZsfzVV goo.gl/SKBGs9	goo.gl/M4lxLS

Xen	CVE-2016-3961 CVE-2016-3157	goo.gl/WivovX goo.gl/LWxxz8	2016-04-14	متوسط	آسیب‌پذیری‌های به دست آوردن اطلاعات حساس، افزایش سطح دسترسی و جلوگیری از سرویس در Xen	وصله برای نسخه‌های 4.5.x الی ماقبل آن : goo.gl/qSrKow وصله برای نسخه‌های 4.4.x و 4.5- rc7 : goo.gl/GHdZYh	goo.gl/bZSbDn goo.gl/iNskhb
Hyper-V	MS16-045	goo.gl/P6VzvT	2016-04-12	متوسط	چندین آسیب‌پذیری اجرای کد از راه دور در Hyper-V در صورت اجرای یک برنامه‌ی کاربردی جعلی توسط مهاجم احراز هویت شده روی سیستم میزبان	برای ویندوز 8.1 64bit : goo.gl/1UPCjC برای ویندوز Server 2012 R2 : goo.gl/W54xWs ویندوز 10 64bit را به‌روزرسانی نمائید. KB3147461	goo.gl/7GDUrm goo.gl/tkvOYz goo.gl/TZkt5C
Citrix XenMobile	CVE-2016-2789	goo.gl/SS1Vmt	2016-03-09	متوسط	آسیب‌پذیری تزریق اسکریپت وب یا HTML در سرویس‌دهنده‌ی Citrix XenMobile به واسطه‌ی وجود XSS در واسط کاربری وب	آسیب‌پذیری فوق در سرویس‌دهنده‌ی Citrix XenMobile نسخه‌های 10.1 Rolling Patch 4 و 10.3 Rolling Patch 1 برطرف گردیده است. goo.gl/P80S5v goo.gl/flzzy7	goo.gl/rkVIhi
Citrix Command Center	CVE-2015-7999	goo.gl/T258H5	2015-12-16	متوسط	چندین آسیب‌پذیری تزریق SQL در واسط وب مدیریتی Citrix Command Center	آسیب‌پذیری‌های فوق در Citrix Command Center نسخه‌های 5.1 Build 36.7 و 5.2 Build 44.11 برطرف گردیده است. goo.gl/YTKdtL	goo.gl/ueFQ16

Xen	CVE-2016-2271 CVE-2016-2270	goo.gl/O74HSs goo.gl/ANjKv0	2016-02-17		آسیب‌پذیری‌های جلوگیری از سرویس و راه‌اندازی مجدد در کلیه‌ی نسخه‌های Xen	وصله برای نسخه‌های 4.6.x : goo.gl/EmhNtC goo.gl/xEqhMG وصله برای نسخه‌های 4.5.x : goo.gl/Rj4buf goo.gl/KGs6T4 وصله برای نسخه‌های 4.4.x : goo.gl/Rj4buf goo.gl/RRpq0K	goo.gl/jFu1mQ goo.gl/zy0yzy
Xen	CVE-2016-1571 CVE-2016-1570	goo.gl/MN3aCa goo.gl/1QSfYm	2016-01-22	زیاد	آسیب‌پذیری به دست آوردن اطلاعات حساس، افزایش سطح دسترسی و جلوگیری از سرویس در Xen به واسطه‌ی وجود نقص در قابلیت PV superpage و تابع paging_invlpg	وصله برای کلیه‌ی نسخه‌های 4.6.x، 4.5.x، 4.4.x و 4.3.x : goo.gl/nSljms وصله برای نسخه‌های 4.6.x و 4.5.x : goo.gl/sno6tv وصله برای نسخه‌های 4.4.x و 4.3.x : goo.gl/uJDvWA	goo.gl/FbmZro goo.gl/syCDtm
QEMU	CVE-2015-7512	goo.gl/xqWLUv	2016-01-14	متوسط	آسیب‌پذیری جلوگیری از سرویس و اجرای کد از راه دور در QEMU به علت سرریزی بافر در تابع pcnet_receive	برای رفع این آسیب‌پذیری در QEMU نسخه‌ی 2.5 وصله‌ی زیر را نصب نمائید. goo.gl/p8Gsw2	goo.gl/Bfafgj

VMware	CVE-2015-6933	goo.gl/EJQp6D	2016-01-07	متوسط	آسیب‌پذیری جلوگیری از سرویس و افزایش سطح دسترسی در نسخه‌های مختلف VMware Workstation، VMware Player، VMware Fusion و VMware ESXi به علت نقص در پیاده‌سازی VMware Tools	آسیب‌پذیری فوق در VMware Workstation نسخه‌ی 11.1.2، VMware Player نسخه‌ی 7.1.2 و VMware Fusion نسخه‌ی 7.1.2 برطرف گردیده است. برای برطرف شدن این آسیب‌پذیری در VMware ESXi نسخه‌های 5.5 و 6.0 باید به ترتیب وصله‌های ESXi550-201512102-SG و ESXi600-201601102-SG نصب گردند. goo.gl/HeHqMI	goo.gl/SA7Sbh

تجهیزات شبکه، دیواره‌های آتش و ضدبدافزار

موضوع	شناسه	منبع	تاریخ انتشار	سطح خطر	خلاصه‌ای از آسیب‌پذیری	نحوه رفع	اطلاعات بیشتر
Cisco	CVE-2016-1376	goo.gl/F0zKsG	2016-04-20	متوسط	آسیب‌پذیری جلوگیری از سرویس در Cisco IOS نسخه‌های 4.2.3، 4.3.0، 4.3.4 و 5.3.1 روی مسیریاب‌های ASR 9000 با استفاده از بسته‌های جعلی	آسیب‌پذیری فوق در Cisco IOS نسخه‌های نرم‌افزاری 5.2.4.SP3، 5.3.2.SP2، 5.3.3.14i و 6.0.0.19i برطرف گردیده است. goo.gl/4io7bp	goo.gl/kwA0xz
Juniper	CVE-2016-1274 CVE-2016-1273 CVE-2016-1271	goo.gl/NMUftJ goo.gl/uoLyL5 goo.gl/ocd6bf , …	2016-04-15	زیاد	چندین آسیب‌پذیری شکستن سازوکار رمزنگاری و احراز هویت، افزایش سطح دسترسی، تغییرات در فایل‌ها و جلوگیری از سرویس در سیستم عامل Junos	آسیب‌پذیری‌های فوق در نسخه‌های به‌روز سیستم عامل Jounos برطرف گردیده است. goo.gl/Fstzfo	goo.gl/I5J80J goo.gl/uUtMRU goo.gl/DW1tih
ESET NOD32	CVE-2015-8841	goo.gl/67tPAA	2016-04-11	----	آسیب‌پذیری اجرای کد از راه دور در ESET NOD32 به واسطه‌ی وجود سریزی بافر مبتنی بر هیپ در ماژول Archive support هنگام باز شدن فایل نصبی EPOC	آسیب‌پذیری فوق در ESET NOD32 در به‌روزرسانی 11861 برطرف گردیده است.	goo.gl/PFfXsM

Sophos UTM	CVE-2016-3968	goo.gl/DykA9e	2016-04-05	متوسط	آسیب‌پذیری XSS در تجهیزات UTM شرکت Sophos مدل‌های CR100iNG با نسخه‌ی نرم‌افزاری 10.6.3 MR-1 build 503 و CR35iNG با نسخه‌های نرم‌افزاری 10.6.2 MR-1 build 383 و 10.6.2 Build 378	تاکنون راه حلی برای این آسیب‌پذیری ارائه نگردیده است.	goo.gl/xcqdvm
FortiOS	CVE-2016-3978	goo.gl/TCNjX3	2016-03-16	کم	آسیب‌پذیری‌های XSS و تغییر مسیر کاربر به وب‌سایت دلخواه در FortiOS با استفاده از پارامتر redirect هنگام ورود به سیستم	آسیب‌پذیری‌های فوق در FortiOS نسخه‌های 5.4.0، 5.2.3 و 5.0.13 برطرف گردیده است. نسخه‌های 4.3 و ماقبل آن، آسیب‌پذیر نیستند.	goo.gl/UPpXuO
Avast	CVE-2015-8620 CVE-2016-3986	goo.gl/5o8VJN goo.gl/rW2dtt	2016-02-24	زیاد	آسیب‌پذیری‌های افزایش سطح دسترسی و جلوگیری از سرویس در Avast به واسطه‌ی وجود سرریزی بافر مبتنی بر هیپ در aswSnx.sys و نیز وقوع خرابی حافظه	آسیب‌پذیری با شناسه‌ی CVE-2015-8620 در Avast نسخه‌ی 11.1.2253 برطرف گردیده است. هنوز راه حلی برای آسیب‌پذیری با شناسه‌ی CVE-2016-3986 ارائه نگردیده است.	goo.gl/s9bV1O goo.gl/ovKoJx
McAfee ATD	CVE-2016-3983	goo.gl/43UNTk	2016-02-16	زیاد	آسیب‌پذیری دور زدن سازوکار تشخیص بدافزار در McAfee Advanced Threat Defense	آسیب‌پذیری فوق در McAfee Advanced Threat Defense نسخه‌ی 3.4.8.178 برطرف گردیده است. goo.gl/5yqVa	goo.gl/tdAg9o
Cisco	CVE-2015-3197 CVE-2016-0701	goo.gl/jxyz4g	2016-03-24	زیاد	چندین آسیب‌پذیری در برخی از محصولات Cisco به علت شکسته شدن سازوکار رمزنگاری و آشکارسازی اطلاعات حساس در OpenSSL	تاکنون راه حلی برای رفع آسیب‌پذیری فوق ارائه نگردیده است.	goo.gl/jxyz4g
Symantec Endpoint Protection	CVE-2015-8154 CVE-2015-8153 CVE-2015-8152	goo.gl/IFYXu6	2016-03-17	زیاد	آسیب‌پذیری‌های اجرای کد از راه دور، تزریق SQL، ربودن احراز هویت مدیر و افزایش سطح دسترسی در Symantec Endpoint Protection نسخه‌ی 12.1	آسیب‌پذیری‌های فوق در Symantec Endpoint Protection نسخه‌ی 12.1 RU6-MP4 برطرف گردیده است. goo.gl/rFEaNN	goo.gl/AvpYU2 goo.gl/WFXlin goo.gl/w2W4jZ

Cisco	CVE-2016-1312	goo.gl/GWzOrz	2016-03-09	زیاد	آسیب‌پذیری خرابی حافظه و جلوگیری از سرویس در محصولات Cisco ASA 5500 سری -CSC SSM با نسخه‌های نرم‌افزاری 6.6 الی ماقبل 6.6.1164.0 با استفاده از ارسال سیل‌آسای بسته‌های HTTPS	آسیب‌پذیری فوق در محصولات Cisco ASA 5500 سری -CSC SSM با نسخه‌های نرم‌افزاری 6.6(1157) و 6.6(1164) برطرف گردیده است. نسخه‌های 6.1، 6.2 و 6.3 آسیب‌پذیر نیستند. goo.gl/XiA01L	goo.gl/sy3WPZ
HP Support Assistant	CVE-2016-2245	goo.gl/QWvKNd	2016-03-04	زیاد	آسیب‌پذیری دور زدن سازوکار احراز هویت در HP Support Assistant	این آسیب‌پذیری در HP Support Assistant نسخه‌ی 8.1.52.1 برطرف گردیده است. goo.gl/Zn7si	goo.gl/Gnxlz8

نرم‌افزارهای کاربردی

موضوع	شناسه	منبع	تاریخ انتشار	سطح خطر	خلاصه‌ای از آسیب‌پذیری	نحوه رفع	اطلاعات بیشتر
giflib	CVE-2016-3977	goo.gl/XRGp1Q	2016-04-21	----	آسیب‌پذیری جلوگیری از سرویس در giflib به واسطه‌ی وجود سرریزی بافر مبتنی بر هیپ در gif2rgb.c با استفاده از یک فایل GIF جعلی	آسیب‌پذیری فوق در openSUSE برطرف گردیده است. goo.gl/hUXdrp	goo.gl/XRGp1Q
libssh	CVE-2016-0739 CVE-2015-3146	goo.gl/f5rzll goo.gl/rSzQzD	2016-04-13	زیاد	آسیب‌پذیری‌های قطع و یا رمزگشایی نشست SSH و جلوگیری از سرویس در libssh	آسیب‌پذیری‌های فوق در Ubuntu برطرف گردیده است. goo.gl/KwqsaL	goo.gl/75I7xC goo.gl/ocXCQX
LibTIFF	CVE-2015-8784 CVE-2015-8783 CVE-2015-8782 , …	goo.gl/gyfkHx goo.gl/Eabn66 goo.gl/f55S57 , …	2016-04-13	متوسط	چندین آسیب‌پذیری جلوگیری از سرویس در LibTIFF با استفاده از یک تصویر TIFF جعلی	آسیب‌پذیری‌های فوق در Debian برطرف گردیده است. goo.gl/ik5eFH	goo.gl/AZdFMD goo.gl/Ntpxm8 goo.gl/b42Xfu , …

Microsoft Office	MS16-042	goo.gl/sz9pSP	2016-04-12	زیاد	چنـدین آسـیب‌پـذیری اجـرای کـد از راه دور در محصـولات Microsoft Office در صـورت بـاز کردن یک فایل Office جعلی در ویندوز و مک	برای Microsoft Office 2010 SP2 32bit : goo.gl/KqQJnv goo.gl/CJvN4N goo.gl/5hihVG برای Microsoft Office 2016 64bit روی مک : goo.gl/HzcmzW	goo.gl/sz9pSP
Adobe Flash Player	APSB16-10	goo.gl/rDxx9c	2016-04-12	زیاد	چندین آسیب‌پذیری دور زدن محدودیت‌های امنیتی، اجرای کد دلخواه، افـزایش سـطح دسترسـی، خرابـی حافظه و جلـوگیری از سـرویس در Adobe Flash Player، Adobe AIR SDK و Adobe AIR SDK & Compiler در سیستم‌های عامل ویندوز، لینوکس، مک، اندروید و iOS	ایـن آسـیب‌پـذیری‌هـا در Adobe Flash Player نسـخه‌هـای 18.0.0.343 و 21.0.0.213 در ویننـدوز و مـک، نسـخه‌ی 11.2.202.616 در لینـوکس و در Adobe AIR SDK و Adobe AIR SDK & Compiler نسـخه‌ی 21.0.0.198 برطـرف گردیده است. goo.gl/qDW9E goo.gl/7nCY goo.gl/2NP5Y مرورگرهـای Internet Explorer و Google Chrome را بـه‌روزرسـانی کنید. ویندوز 10 را به‌روزرسانی نمائید.	goo.gl/SWOvL5 goo.gl/uUPhpb goo.gl/VbjjBu , …
NVIDIA	CVE-2016-2558 CVE-2016-2557 CVE-2016-2556	goo.gl/sJ7QZh goo.gl/eIDTkx goo.gl/xIEFEX	2016-04-12	----	آسیب‌پذیری‌های به دست آوردن اطلاعـات حسـاس، افزایش سـطح دسترسـی و جلـوگیری از سـرویس در درایور گرافیک NVIDIA در ویندوز	این آسیب‌پذیری‌ها در درایور گرافیـک NVIDIA نسخه‌هـای R341.95 و R354.74 برطرف گردیده است. goo.gl/LGhxO	goo.gl/S1N48a goo.gl/ZUTH5Y goo.gl/HCmLa8
BeanShell (bsh)	CVE-2016-2510	goo.gl/AR5P79	2016-04-12	----	آسیب‌پذیری اجرای کد دلخـواه در پوسـته‌ی bsh بـا استفاده از داده‌های سری شده‌ی جعلی	آسیب‌پـذیری فـوق در پوسـته‌ی bsh نسخه‌ی 2.0b6 برطرف گردیده است. goo.gl/vj1lPi	goo.gl/MA05gz

PuTTY, KiTTY	CVE-2016-2563	goo.gl/SCz5DO	2016-04-11	زیاد	آسیب‌پذیری جلوگیری از سرویس در ابزارهای PuTTY و KiTTY به واسطه‌ی خرابی حافظه در اثر وجود سرریزی بافر مبتنی بر Stack	آسیب‌پذیری فوق در PuTTY نسخه‌ی 0.67 و در KiTTY نسخه‌ی 0.66.6.3 برطرف گردیده است. goo.gl/XbTF goo.gl/wx4psX	goo.gl/dxGd6n
libxml2	CVE-2015-8806 CVE-2015-8710	goo.gl/8qh8VK goo.gl/XkFnDR	2016-04-01	متوسط	آسیب‌پذیری‌های به دست آوردن اطلاعات حساس و جلوگیری از سرویس در libxml2 به واسطه‌ی وجود نقص در فایل‌های dict.c و HTMLparser.c	آسیب‌پذیری با شناسه‌ی CVE-2015-8710 در Debian برطرف گردیده است. هنوز راه حلی برای آسیب‌پذیری با شناسه‌ی CVE-2015-8806 ارائه نگردیده است. goo.gl/oxIiUU	goo.gl/vVBxms goo.gl/X7r02l
PostgreSQL	CVE-2016-3065 CVE-2016-2193	goo.gl/z6b34a	2016-03-31	زیاد	آسیب‌پذیری‌های دور زدن محدودیت‌های امنیتی، به دست آوردن اطلاعات حساس و جلوگیری از سرویس در PostgreSQL نسخه‌های ماقبل 9.5.2	آسیب‌پذیری‌های فوق در PostgreSQL نسخه‌ی 9.5.2 برطرف گردیده است. goo.gl/4WNvi	goo.gl/0JiQW7 goo.gl/8HHt8b
Foxit Reader	----	goo.gl/FhigkI	2016-03-16	----	آسیب‌پذیری اجرای کد از راه دور در Foxit Reader و Foxit PhantomPDF نسخه‌های 7.3.0.118 و ماقبل آن	آسیب‌پذیری فوق در Foxit Reader و Foxit PhantomPDF نسخه‌ی 7.3.4.0311 برطرف گردیده است. goo.gl/1UgGb5	goo.gl/FhigkI
Libpng	CVE-2015-8540	goo.gl/pk9gba	2016-02-24	زیاد	آسیب‌پذیری‌های اجرای کد از راه دور و جلوگیری از سرویس در libpng به واسطه‌ی سرریزی مقدار عدد صحیح در pngwutil.c با استفاده از یک فایل PNG جعلی	آسیب‌پذیری‌های فوق در libpng نسخه‌های 1.0.66، 1.2.56، 1.4.19 و 1.5.26 برطرف گردیده است. goo.gl/vt4ub	goo.gl/SeMgCq

Adobe Flash Player	APSB16-08	goo.gl/0W2gJU	2016-03-10	زیاد	چندین آسیب‌پذیری اجرای کد دلخواه، خرابی حافظه و جلوگیری از سرویس در Adobe Flash Player، Adobe AIR SDK و Adobe AIR SDK & Compiler در سیستم‌های عامل ویندوز، لینوکس، مک، اندروید و iOS	این آسیب‌پذیری‌ها در Adobe Flash Player نسخه‌های 18.0.0.333 و 21.0.0.182 در ویندوز و مک، نسخه‌ی 11.2.202.577 در لینوکس و در Adobe AIR SDK و Adobe AIR SDK & Compiler نسخه‌ی 21.0.0.176 برطرف گردیده است. goo.gl/qDW9E goo.gl/7nCY goo.gl/2NP5Y مرورگرهای Internet Explorer و Google Chrome را به‌روزرسانی کنید. ویندوز 10 را به‌روزرسانی نمائید.	goo.gl/BwV5fE goo.gl/ebEvRt goo.gl/SBuf49 , …
Apple Software Update	CVE-2016-1731	goo.gl/jGD6xM	2016-03-10	متوسط	آسیب‌پذیری به‌روزرسانی‌های جعلی در Apple Software Update روی ویندوز به واسطه‌ی عدم استفاده از HTTPS و امکان حمله‌ی MitM	آسیب‌پذیری فوق در Apple Software Update نسخه‌ی 2.2 برطرف گردیده است. goo.gl/XQWbH	goo.gl/z7uHXk