

جدول آخرین به روز رسانی ها و آسیب پذیری های نرم افزارهای پر کاربرد در کشور

سرویس دهنده ها (وب، پست الکترونیک، پراکسی و غیره)

دریافت آخرین نسخه ی پایدار

موضوع	آخرین نسخه ی پایدار	تاریخ عرضه	لینک دریافت
Apache Web Server	2.4.23	2016-07-05	goo.gl/ySdR
Squid Proxy & Cache Server	3.5.20	2016-07-01	goo.gl/ZCyZ6f

آسیب پذیری ها

موضوع	شناسه	منبع	تاریخ انتشار	سطح خطر	خلاصه ای از آسیب پذیری	نحوه رفع	اطلاعات بیشتر
Apache HTTP Server	CVE-2016-5387	goo.gl/F990Go	2016-07-19	زیاد	آسیب پذیری تغییر مسیر ترافیک HTTP یک برنامه ی کاربردی به یک سرویس دهنده ی پراکسی دلخواه در Apache HTTP Server توسط مهاجمین MitM	برای آسیب پذیری فوق وصله ی زیر منتشر شده است. goo.gl/F990Go	goo.gl/grqQFF
ISC BIND	CVE-2016-2775	goo.gl/RJsNID	2016-07-18	متوسط	آسیب پذیری جلوگیری از سرویس در ISC BIND در صورت پیکربندی lwresd در پذیرش ارتباط راه دور کلاینت ها	آسیب پذیری فوق در ISC BIND نسخه های 9.10.4-P2، 9.9.9-P2 و 9.11.0b2 برطرف شده است. goo.gl/KQtfv0	goo.gl/sVgyQS
Active Directory	MS16-081	goo.gl/mcGRBD	2016-06-14	متوسط	آسیب پذیری جلوگیری از سرویس در Active Directory در صورت ایجاد چند اکانت توسط مهاجم احراز هویت شده (این مهاجم می بایست دسترسی لازم جهت Join ماشین به دامنه را داشته باشد)	برای ویندوز Server 2008 R2 SP1 64bit : goo.gl/VkdNyo برای ویندوز Server 2012 : goo.gl/w0VIyt	goo.gl/h1lRh1

Microsoft Exchange	MS16-079	goo.gl/izSSCI	2016-06-14	متوسط	چندین آسیب‌پذیری آشکارسازی اطلاعات در سرویس‌دهنده‌ی Microsoft Exchange با ارسال یک آدرس URL عکس جعلی به OWA	برای سرویس‌دهنده‌ی Microsoft Exchange 2010 : goo.gl/SgR15P برای سرویس‌دهنده‌ی Microsoft Exchange 2016 CU1 : goo.gl/vM6eOT	goo.gl/izSSCI
Windows DNS Server	MS16-071	goo.gl/jCGjQL	2016-06-14	زیاد	آسیب‌پذیری اجرای کد از راه دور در Windows DNS Server با استفاده از ارسال درخواست‌های جعلی به سمت سرویس‌دهنده	برای ویندوز Server 2012 : goo.gl/CgLEPE برای ویندوز Server 2012 R2 (Core) : goo.gl/srNGhl	goo.gl/lGcJk3
nginx	CVE-2016-4450	goo.gl/HB2uXU	2016-05-31	زیاد	آسیب‌پذیری جلوگیری از سرویس در nginx نسخه‌های 1.3.9 الی 1.11.0 به واسطه‌ی نقص در عملکرد فایل ngx_files.c هنگام نوشتن بدنه‌ی درخواست کلاینت در یک فایل موقت	آسیب‌پذیری فوق در nginx نسخه‌های 1.11.1 و 1.10.1 برطرف شده است. goo.gl/xQFZy وصله برای nginx نسخه‌های 1.9.13 الی 1.11.0 : goo.gl/wq1tyb وصله برای nginx نسخه‌های 1.3.9 الی 1.9.12 : goo.gl/LZv2LV	goo.gl/QeyA6t

سیستم‌های عامل

موضوع	شناسه	منبع	تاریخ انتشار	سطح خطر	خلاصه‌ای از آسیب‌پذیری	نحوه رفع	اطلاعات بیشتر
Apple iOS, OS X, Safari, tvOS, watchOS	CVE-2016-4653 CVE-2016-4652 CVE-2016-4651 , ...	goo.gl/xelNEV goo.gl/Q1Gocf goo.gl/04w9PV , ...	2016-07-18	زیاد	آسیب‌پذیری‌های افزایش سطح دسترسی، XSS، به‌دست آوردن اطلاعات حساس، اجرای کد از راه دور و جلوگیری از سرویس در محصولات Apple	این آسیب‌پذیری‌ها در Apple iOS نسخه‌ی 9.3.3، Apple OS X نسخه‌ی 10.11.6، tvOS نسخه‌ی 2.2.2، watchOS نسخه‌ی 2.2.2 و Apple Safari نسخه‌ی 9.1.2 برطرف شده است.	goo.gl/3mofUy goo.gl/n01gD4 goo.gl/fcKJWX , ...

goo.gl/BD0kJo goo.gl/AuwSjX goo.gl/duMK3Z , ...	آسیب‌پذیری CVE-2016-3818 در Android نسخه‌ی 4.4.4 و سایر آسیب‌پذیری‌ها در Android نسخه‌ی 2016-07-05 برطرف گردیده‌اند.	چندین آسیب‌پذیری جلوگیری از سرویس، به دست آوردن اطلاعات حساس و افزایش سطح دسترسی در Android	متوسط	2016-07-14	goo.gl/b9V0z8	CVE-2016-3818 CVE-2016-3816 CVE-2016-3815 , ...	Android
goo.gl/n27SvA	برای ویندوز 8.1 32bit : goo.gl/wXjo96 برای ویندوز Server 2012 R2 : goo.gl/N5uayy ویندوز 10 را به‌روزرسانی نمائید. KB3163912 KB3172985	آسیب‌پذیری دورزدن محدودیت امنیتی Secure Boot در ویندوز در صورت دسترسی مهاجم به سیستم قربانی و نصب یک Policy جعلی	متوسط	2016-07-12	goo.gl/gGLXzs	MS16-094	Windows
goo.gl/fCcPHp	برای ویندوز 8.1 64bit : goo.gl/g9jQ0x برای ویندوز Server 2012 R2 : goo.gl/uRWHX9 ویندوز 10 را به‌روزرسانی نمائید. KB3174060	چندین آسیب‌پذیری در Adobe Flash Player در ویندوز	زیاد	2016-07-12	goo.gl/fCcPHp	MS16-093	Windows
goo.gl/jlhFLN goo.gl/GvnfJg	برای ویندوز 8.1 64bit : goo.gl/9ddY6Q goo.gl/BLT4gi برای ویندوز Server 2012 R2 : goo.gl/U33ALR goo.gl/a8YIk5 ویندوز 10 را به‌روزرسانی نمائید. KB3163912 KB3172985	چندین آسیب‌پذیری دورزدن محدودیت‌های امنیتی در ویندوز به واسطه‌ی عدم موفقیت هسته‌ی ویندوز در تعیین چگونگی استفاده از ویژگی‌های مدیریت شیء توسط برنامه‌ی کاربردی	متوسط	2016-07-12	goo.gl/CwSBMt	MS16-092	Windows
goo.gl/NkagjE	برای ویندوز 7 SP1 64bit : goo.gl/swR1EW برای ویندوز Server 2012 R2 : goo.gl/ccSdh4 ویندوز 10 را به‌روزرسانی نمائید. KB3163912 KB3172985	چندین آسیب‌پذیری افزایش سطح دسترسی و آشکارسازی اطلاعات در ویندوز در صورت ورود مهاجم به سیستم قربانی و اجرای یک برنامه‌ی کاربردی جعلی	متوسط	2016-07-12	goo.gl/NkagjE	MS16-090	Windows

goo.gl/O6DOoQ	ویندوز 10 را به روزرسانی نمائید. KB3163912 KB3172985	آسیب پذیری آشکار سازی اطلاعات در ویندوز به واسطه ی عدم مدیریت صحیح اشیاء در حافظه توسط Windows Secure Kernel Mode	متوسط	2016-07-12	goo.gl/QfdgQP	MS16-089	Windows
goo.gl/VcHKvi goo.gl/J5o1X7	روی ویندوز 7 SP1 32bit : goo.gl/J1G5lh روی ویندوز Server 2012 R2 : goo.gl/DROkPx ویندوز 10 را به روزرسانی نمائید. KB3163912 KB3172985	چندین آسیب پذیری اجرای کد از راه دور در ویندوز به واسطه ی امکان حمله ی MitM روی یک سیستم کلاینت یا سرویس دهنده ی چاپ ناشی از نقص در سرویس Print Spooler	زیاد	2016-07-12	goo.gl/rsBQWD	MS16-087	Windows
goo.gl/n4NHD4 goo.gl/EntpJH	برای VBScript 5.7 روی ویندوز Server 2008 32bit (GUI & Core) : goo.gl/aF1Is3 برای VBScript و JScript 5.8 روی ویندوز Server 2008 R2 : SP1 64bit (Core) goo.gl/IqNbn1	آسیب پذیری های اجرای کد از راه دور و افزایش سطح دسترسی در موتورهای JScript و VBScript در سیستم های عامل ویندوز Vista، Server 2008 و Server 2008 R2 در صورت مشاهده ی یک صفحه ی وب جعلی	زیاد	2016-07-12	goo.gl/i2u0ST	MS16-086	Windows

محیط های برنامه نویسی

دریافت آخرین نسخه ی پایدار

لینک دریافت	تاریخ عرضه	آخرین نسخه پایدار	موضوع
goo.gl/ZEG0Nh	2016-08-04	3.6.2	Joomla!
goo.gl/c5F8At	2016-08-03	8.1.8	Drupal
goo.gl/DK0Wx	2016-06-18	4.5.3	WordPress
goo.gl/pT76iH	2016-05-26	8.00.03	DotNetNuke

آسیب پذیری ها

موضوع	شناسه	منبع	تاریخ انتشار	سطح خطر	خلاصه ای از آسیب پذیری	نحوه رفع	اطلاعات بیشتر
Perl	CVE-2016-6185 CVE-2016-1238	goo.gl/DP4yy0 goo.gl/C4Mv3U	2016-07-25	زیاد	آسیب پذیری های افزایش سطح دسترسی و اجرای کد دلخواه در Perl به واسطه ی عدم پاک سازی صحیح کاراکتر . از انتهای آرایه ی دایرکتوری includes (@INC) و عدم عملکرد مناسب XSLoader	آسیب پذیری افزایش سطح دسترسی در Perl نسخه های 5.22.3-RC2 و 5.24.1-RC2 برطرف شده است. برای رفع آسیب پذیری اجرای کد دلخواه تاکنون راه حلی ارائه نشده است.	goo.gl/cbHwDT goo.gl/kmw2so
PHP	CVE-2016-6297 CVE-2016-6296 CVE-2016-6295 , ...	goo.gl/Giyf7V goo.gl/gxRMn4 goo.gl/nYsrRp , ...	2016-07-25	زیاد	چندین آسیب پذیری جلوگیری از سرویس در PHP به واسطه ی وجود سرریزی بافر مبتنی بر Stack، سرریزی بافر مبتنی بر هیپ، خرابی حافظه و غیره	آسیب پذیری های فوق در PHP نسخه ی 5.5.38، 5.6.24 و 7.0.9 برطرف شده است. goo.gl/DGeo	goo.gl/bxznLp goo.gl/zLGxt0 goo.gl/5IzzFr , ...
ASN1C	CVE-2016-5080	goo.gl/Hp0vXK	2016-07-19	زیاد	آسیب پذیری های اجرای کد دلخواه و جلوگیری از سرویس در کامپایلر ASN1C برای C/C++ به واسطه ی وجود سرریزی بافر مبتنی بر هیپ با استفاده از داده های ASN.1 جعلی	برای رفع آسیب پذیری های فوق وصله ی منتشر شده برای ASN1C نسخه های 7.0.1.x را نصب کنید و یا از نسخه ی 7.0.2 استفاده نمایید. goo.gl/MZinjW	goo.gl/k3Yj87
.NET Framework	MS16-091	goo.gl/yDE8A7	2016-07-12	متوسط	آسیب پذیری آشکار سازی اطلاعات در .NET Framework در صورت بارگذاری یک فایل XML جعلی به یک برنامه ی کاربردی مبتنی بر وب	برای .NET Framework 3.5.2 روی سیستم های عامل ویندوز 7 و SP1 32bit، SP1 64bit و Server 2008 R2 SP1 64bit : goo.gl/oVFnhv ویندوز 10 را به روز رسانی نمایید. KB3163912 KB3172985	goo.gl/Tj4PxD

goo.gl/LN1C26 goo.gl/OgtvNT goo.gl/rAbj9C , ...	آسیب‌پذیری‌های فوق در WordPress نسخه 4.5.3 برطرف شده است. goo.gl/DK0Wx	چندین آسیب‌پذیری XSS، آشکارسازی اطلاعات حساس، جلوگیری از سرویس، تغییر کلمه عبور و غیره در WordPress	زیاد	2016-06-18	goo.gl/TE1qdg	CVE-2016-5839 CVE-2016-5838 CVE-2016-5837 , ...	WordPress
---	---	---	------	------------	--	--	-----------

مرورگرهای اینترنت

دریافت آخرین نسخه پایدار

موضوع	آخرین نسخه پایدار	تاریخ عرضه	لینک دریافت
Mozilla Firefox	48.0	2016-08-02	goo.gl/yIXtW
Google Chrome	52.0.2743.116	2016-08-04	goo.gl/Jk2diZ

آسیب‌پذیری‌ها

موضوع	شناسه	منبع	تاریخ انتشار	سطح خطر	خلاصه‌ای از آسیب‌پذیری	نحوه رفع	اطلاعات بیشتر
Mozilla Firefox, ESR	CVE-2016-5268 CVE-2016-5267 CVE-2016-5266 , ...	goo.gl/g5W3ES goo.gl/1h5bFU goo.gl/RFL2Tu , ...	2016-08-02	متوسط	چندین آسیب‌پذیری XSS، جعل آدرس، افزایش سطح دسترسی، دورزدن محدودیت‌های امنیتی، اجرای کد از راه دور، جلوگیری از سرویس و غیره در مرورگر Mozilla Firefox و Firefox ESR	آسیب‌پذیری‌های فوق در مرورگر Mozilla Firefox نسخه 48.0 و در Firefox ESR نسخه 45.3 برطرف شده است. goo.gl/yIXtW goo.gl/8WbxPl	goo.gl/NCUOCZ goo.gl/Qw8NEe goo.gl/WYn6Xb , ...
Google Chrome	CVE-2016-5138	goo.gl/bM4sIO	2016-08-01	متوسط	آسیب‌پذیری جلوگیری از سرویس در مرورگر Google Chrome به واسطه‌ی وجود سرریزی مقدار عدد ص 16 حیح در تابع kbasep_vinstr_attach_client	آسیب‌پذیری فوق در مرورگر Google Chrome نسخه 52.0.2743.85 برطرف شده است. goo.gl/Jk2diZ	goo.gl/YeLybH

goo.gl/1fLfHK	KB3163912 KB3172985 ویندوز 10 را به روزرسانی نمائید.	چندین آسیب پذیری اجرای کد از راه دور و افزایش سطح دسترسی در مرورگر Microsoft Edge در صورت مشاهده ی یک صفحه ی وب جعلی	زیاد	2016-07-12	goo.gl/1fLfHK	MS16-085	Microsoft Edge
goo.gl/00jk8N	Internet Explorer برای مرورگر نسخه ی 11 روی : ویندوز 7 SP1 64bit : goo.gl/lfbDh9 ویندوز Server 2012 R2 : goo.gl/6MVlux ویندوز 10 را به روزرسانی نمائید. KB3163912 KB3172985	چندین آسیب پذیری اجرای کد از راه دور، افزایش سطح دسترسی، ایجاد تغییرات در فایل ها و غیره در Internet Explorer در صورت مشاهده ی یک صفحه ی وب جعلی	زیاد	2016-07-12	goo.gl/00jk8N	MS16-084	Internet Explorer
goo.gl/N5Iri2 goo.gl/86GE4n goo.gl/s6VuN6 , ...	آسیب پذیری های فوق در مرورگر Mozilla Firefox نسخه ی 47.0 و در Firefox ESR نسخه ی 45.2 برطرف شده است. goo.gl/yIXtW	چندین آسیب پذیری XSS، اجرای کد از راه دور، به دست آوردن اطلاعات حساس، دورزدن محدودیت های امنیتی، جلوگیری از سرویس و غیره در مرورگر Mozilla Firefox و Firefox ESR	متوسط	2016-06-07	goo.gl/nRQ33v goo.gl/CjtQHZ goo.gl/x6VXrX , ...	CVE-2016-2834 CVE-2016-2833 CVE-2016-2832 , ...	Mozilla Firefox, ESR

مجازی سازی

دریافت آخرین نسخه ی پایدار

موضوع	آخرین نسخه پایدار	تاریخ عرضه	لینک دریافت
VirtualBox	5.1.2	2016-07-21	goo.gl/l3wrf

آسیب پذیری ها

موضوع	شناسه	منبع	تاریخ انتشار	سطح خطر	خلاصه ای از آسیب پذیری	نحوه رفع	اطلاعات بیشتر
-------	-------	------	--------------	---------	------------------------	----------	---------------

goo.gl/0vkjYw goo.gl/rMH9BJ	وصله برای نسخه‌های 4.7.x و : unstable goo.gl/h8j8Ce goo.gl/qAqwJT سایر وصله‌ها در لینک‌های زیر : goo.gl/Foo4Sf goo.gl/BVt7AF	آسیب‌پذیری‌های جلوگیری از سرویس و افزایش سطح دسترسی در نسخه‌های مختلف Xen	زیاد	2016-07-26	goo.gl/Foo4Sf goo.gl/BVt7AF	CVE-2016-6259 CVE-2016-6258	Xen
goo.gl/ho1U4D goo.gl/tt6vhO goo.gl/kTvYHU	برای رفع آسیب‌پذیری‌های فوق می‌بایست وصله‌ی منتشر شده نصب گردد. goo.gl/zNP6rb	آسیب‌پذیری‌های به دست آوردن کلمه‌ی عبور، افزایش سطح دسترسی و اجرای کد از راه دور در SolarWinds Virtualization Manager نسخه‌ی 6.3.1 به واسطه‌ی رمزنگاری ضعیف هنگام ذخیره‌سازی کلمات عبور در /etc/shadow و نقص در سرویس RMI	زیاد	2016-06-16	goo.gl/k1Quhy goo.gl/IYc7zc goo.gl/9CJfaZ	CVE-2016-5709 CVE-2016-3643 CVE-2016-3642	SolarWinds Virtualization Manager
goo.gl/rzxFgd	این آسیب‌پذیری در سرویس‌دهنده‌ی Vmware vCenter نسخه‌های 5.5 U2d و 5.1 U3d، 5.0 U3g برطرف شده است. goo.gl/JM7Bmp goo.gl/vejqcH goo.gl/1hYvqD نسخه‌ی 6.0 متاثر از این آسیب‌پذیری نیست.	آسیب‌پذیری XSS در vSphere Web Client در سرویس‌دهنده‌ی VMware vCenter به واسطه‌ی عدم پاک‌سازی ورودی به طور مناسب با استفاده از ترغیب قربانی به کلیک کردن روی یک لینک مخرب	متوسط	2016-06-14	goo.gl/sdp85O	CVE-2015-6931	VMware vCenter
goo.gl/5xLik5	این آسیب‌پذیری در صورت نصب وصله‌ی XS70E003 برطرف می‌گردد.	آسیب‌پذیری افزایش سطح دسترسی در Citrix XenServer توسط کاربران اکتیو دایرکتوری احراز هویت شده در صورت به‌روزرسانی نسخه‌های پیشین به آخرین نسخه	زیاد	2016-06-09	goo.gl/Dz5Yiu	CVE-2016-5302	Citrix XenServer

تجهیزات شبکه، دیوارهای آتش و ضدبدافزار

موضوع	شناسه	منبع	تاریخ انتشار	سطح خطر	خلاصه‌ای از آسیب‌پذیری	نحوه رفع	اطلاعات بیشتر
-------	-------	------	-----------------	------------	------------------------	----------	---------------

goo.gl/Ofp62M	آسیب‌پذیری فوق در نسخه‌های نرم‌افزاری 5.2(1)SV3(1.5i) و 5.2(1)SV3(1.6) برطرف شده است. goo.gl/StpkMO	آسیب‌پذیری جلوگیری از سرویس در Cisco Nexus 1000v AVS با نسخه‌های نرم‌افزاری 5.2(1)SV3(2.1) و 5.2(1)SV3(1.5a) از کار افتادن ESXi با استفاده از یک بسته‌ی CDP جعلی	متوسط	2016-07-27	goo.gl/LstFiy	CVE-2016-1465	Cisco Nexus 1000v AVS
goo.gl/k3Yj87	تاکنون راه حلی برای رفع آسیب‌پذیری فوق ارائه نشده است.	آسیب‌پذیری‌های جلوگیری از سرویس و اجرای کد از راه دور در تجهیزات Cisco ASR 5000 با نسخه‌ی نرم‌افزاری 18.8.0 و Cisco VPC به واسطه‌ی آسیب‌پذیری کامپایلر ASN1C	زیاد	2016-07-21	goo.gl/ir9IEEn	CVE-2016-5080	Cisco ASR 5000
goo.gl/rcsTvY goo.gl/VYvqg1	آسیب‌پذیری‌های فوق در Fortinet FortiWeb نسخه‌ی 5.5.3 برطرف شده است. goo.gl/smA9Sv	آسیب‌پذیری‌های تغییر کلمه‌ی عبور مدیر و افزایش سطح دسترسی در Fortinet FortiWeb به واسطه‌ی وجود CSRF و پیمایش مسیر	متوسط	2016-06-23	goo.gl/TG9GLY goo.gl/9tztqV	CVE-2016-5092 CVE-2016-4066	Fortinet
goo.gl/MEK0Nb goo.gl/C0gC52	برای رفع آسیب‌پذیری‌های فوق وصله‌های ذیل باید نصب گردند. برای نسخه‌ی 10 : ow.ly/JrOG3021dyE برای نسخه‌ی 8 : ow.ly/y3IK3021dGH	آسیب‌پذیری‌های خواندن فایل‌های دلخواه و تزریق اسکریپت وب یا HTML در Trend Micro Internet Security نسخه‌های 8 و 10	متوسط	2016-06-21	goo.gl/4368s8 goo.gl/TKX1hv	CVE-2016-1226 CVE-2016-1225	Trend Micro Internet Security
goo.gl/Ak8ope	آسیب‌پذیری فوق در QNAP QTS نسخه‌ی 4.2.1 برطرف شده است. برای به‌روزرسانی به نسخه‌ی فوق، پس از ورود به NAS به عنوان مدیر، گزینه Firmware Update را از Control Panel انتخاب نمایید.	آسیب‌پذیری تزریق اسکریپت وب یا HTML در QNAP QTS نسخه‌های ماقبل 4.2.1 به واسطه‌ی وجود XSS	متوسط	2016-06-17	goo.gl/VkDzXS	CVE-2015-5664	QNAP QTS

نرم‌افزارهای کاربردی

موضوع	شناسه	منبع	تاریخ انتشار	سطح خطر	خلاصه‌ای از آسیب‌پذیری	نحوه رفع	اطلاعات بیشتر
-------	-------	------	--------------	---------	------------------------	----------	---------------

goo.gl/nnndzz goo.gl/qGaXC2	آسیب‌پذیری‌های فوق در WinCC نسخه‌های U10 7.3 و U1 7.4، PCS 7 نسخه‌ی SP1 8.1 SIMATIC WinCC 7.3 U10)، BATCH 8.1 SP1 U9 PCS 7 (OpenPCS 7 8.1 U3 نسخه‌ی 8.2 U1 WinCC 7.4 U1)، و (OpenPCS 7 8.2 U1 WinCC Runtime Pro نسخه‌ی 13 SP1 U9 برطرف شده است.	آسیب‌پذیری‌های اجرای کد از راه دور و آشکارسازی اطلاعات حساس در نرم‌افزارهای کنترل سیستم‌های صنعتی Siemens	زیاد	2016-07-22	goo.gl/iyldsm	CVE-2016-5744 CVE-2016-5743	WinCC, PCS, WinCC Runtime Pro
goo.gl/eIFRIO	برای Microsoft Office 2010 SP2 32bit : goo.gl/RmnZGa goo.gl/4qZVii goo.gl/QdtQG8 goo.gl/mGFQXY goo.gl/amEYOA	چندین آسیب‌پذیری اجرای کد از راه دور در Microsoft Office در صورت باز کردن یک فایل Office جعلی در ویندوز و مک	زیاد	2016-07-12	goo.gl/eIFRIO	MS16-088	Microsoft Office
goo.gl/walGCl	تاکنون راه حلی برای رفع این آسیب‌پذیری‌ها ارائه نشده است.	آسیب‌پذیری‌های اجرای کد از راه دور و جلوگیری از سرویس در libbpg نسخه‌های 0.9.5 الی 0.9.7 به واسطه‌ی نقص در عملکرد تابع restore_tqb_pixels با استفاده از یک تصویر جعلی BPG	زیاد	2016-07-12	goo.gl/AYTBaF	CVE-2016-5637	libbpg

goo.gl/fOVV3M	این آسیب‌پذیری‌ها در Adobe Flash Player 22.0.0.209 و در Adobe Flash Player Extended 18.0.0.366 در ویندوز و مک، نسخه‌ی 11.2.202.632 در لینوکس برطرف شده است. goo.gl/qDW9E مرورگرهای Internet Explorer و Google Chrome را به‌روزرسانی کنید. ویندوزهای 8.1 و 10 را به‌روزرسانی نمائید.	چندین آسیب‌پذیری اجرای کد دلخواه، به دست آوردن اطلاعات حساس و جلوگیری از سرویس در Adobe Flash Player در سیستم‌های عامل ویندوز، لینوکس و مک	زیاد	2016-07-12	goo.gl/tl31Ny	APSB16-25	Adobe Flash Player
goo.gl/pclF5f	آسیب‌پذیری فوق در Acrobat DC و Acrobat Reader DC و نسخه‌های Continuous و Classic به ترتیب در نسخه‌های 15.017.20050 و 15.006.30198 و در Acrobat XI و Reader XI نسخه‌ی 11.0.17 برطرف شده است. goo.gl/9E1Y6	چندین آسیب‌پذیری در Acrobat DC و Acrobat Reader DC نسخه‌های Continuous و Classic و در Acrobat XI و Reader XI	----	2016-07-12	goo.gl/pclF5f	APSB16-26	Adobe Acrobat, Reader
goo.gl/2O6ErI	برای رفع این آسیب‌پذیری می‌بایست وصله زیر نصب گردد. goo.gl/vQzXK7	آسیب‌پذیری‌های جلوگیری از سرویس و اجرای کد در GIMP به واسطه‌ی خرابی حافظه ناشی از بارگذاری یک فایل XCF جعلی	زیاد	2016-07-06	goo.gl/VzuuVK	CVE-2016-4994	GIMP
goo.gl/X6ps90	این آسیب‌پذیری در libvirt نسخه‌ی 2.0.0 برطرف شده است. goo.gl/euHJT	آسیب‌پذیری دورزدن احراز هویت در libvirt هنگام تنظیم کلمه‌ی عبور مدیر سرویس‌دهنده‌ی VNC با یک رشته‌ی خالی به واسطه‌ی عدم بررسی مناسب کلمه‌ی عبور	زیاد	2016-06-30	goo.gl/GGHE8o	CVE-2016-5008	libvirt

goo.gl/qXt4l3	برای رفع این آسیب پذیری می بایست وصله های زیر نصب گردند. goo.gl/tMFszW goo.gl/ZX3vOj	آسیب پذیری دسترسی به اطلاعات حساس در KDE به واسطه ی دسترسی به کوکی های X11 به علت حق دسترسی ضعیف 644 روی -tmp/xauth/ Kinit در xxx-y	زیاد	2016-06-21	goo.gl/Ab87nz	CVE-2016-3100	KDE
goo.gl/9eqqfr goo.gl/bcJLfE goo.gl/dCLSBd ، ...	NTP آسیب پذیری های فوق در نسخه ی 4.2.8p8 برطرف شده است. goo.gl/WcTx2	چندین آسیب پذیری جلوگیری از سرویس در NTP 4.x نسخه های ماقبل 4.2.8p8	متوسط	2016-07-06	goo.gl/FHGtwD goo.gl/pWRKre goo.gl/8vWwpw ، ...	CVE-2016-4957 CVE-2016-4956 CVE-2016-4955 ، ...	NTP
goo.gl/nOV0Dx	LibreOffice آسیب پذیری فوق در نسخه ی 5.1.4 برطرف شده است. goo.gl/FGpA4Y	آسیب پذیری اجرای کد از راه دور در LibreOffice به واسطه ی عدم تجزیه ی مناسب فایل های RTF	زیاد	2016-06-28	goo.gl/w0F8qS	CVE-2016-4324	LibreOffice
goo.gl/19Vw6p goo.gl/Tqni4b goo.gl/PQXVYJ ، ...	آسیب پذیری های فوق در phpMyAdmin نسخه های 4.0.10.16، 4.4.15.7 و 4.6.3 برطرف شده است. goo.gl/j3gQ4B وصله هایی نیز برای نسخه های 4.0.x، 4.4.x و 4.6.x منتشر شده است.	چندین آسیب پذیری CSRF، اجرای کد PHP XSS و غیره در phpMyAdmin	زیاد	2016-06-23	goo.gl/QmjdjE goo.gl/L9EGJs goo.gl/w3L6Mg ، ...	CVE-2016-5739 CVE-2016-5734 CVE-2016-5733 ، ...	phpMyAdmin