

جدول آخرین به روزرسانی ها و آسیب پذیری های نرم افزارهای پرکاربرد 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	3.5.23	2016-12-16	goo.gl/ZCyZ6f

آسیب پذیری ها

موضوع	شناسه	منبع	تاریخ انتشار	سطح خطر	خلاصه ای از آسیب پذیری	نحوه رفع	اطلاعات بیشتر
Microsoft SQL Server	MS16-136	goo.gl/27XbVU	2016-11-08	متوسط	چندین آسیب پذیری افزایش سطح دسترسی و به دست آوردن توانایی مشاهده، تغییرات و یا پاک کردن داده ها در Microsoft SQL Server	برای SQL Server 2012 SP3 : 32, 64bit goo.gl/x0YdS7 برای SQL Server 2014 SP2 : 32, 64bit goo.gl/MKeoY3 برای SQL Server 2016 64bit : goo.gl/cwsutx	goo.gl/27XbVU
ISC BIND	CVE-2016-8864	goo.gl/AwtMEM	2016-11-01	زیاد	آسیب پذیری جلوگیری از سرویس در ISC BIND به واسطه ی نقص در عملکرد db.c و resolver.c با استفاده از یک رکورد DNAME در بخش answer یک پاسخ جستجوی بازگشتی	آسیب پذیری فوق در ISC BIND نسخه های 9.10.4-P4, 9.9.9-P4 و 9.11.0-P1 برطرف گردیده است. goo.gl/E3i9do	goo.gl/QJdi5r

سیستم های عامل

موضوع	شناسه	منبع	تاریخ انتشار	سطح خطر	خلاصه‌ای از آسیب پذیری	نحوه رفع	اطلاعات بیشتر
Windows	MS16-154	goo.gl/a7JJlc	2016-12-13	زیاد	چندین آسیب‌پذیری در Adobe Flash Player در ویندوز	برای ویندوز نسخه‌های 32- 8.1 Server 2012 64bit و 10 RT 8.1 2012 R2 : 2016 goo.gl/W5FpIZ	goo.gl/a7JJlc
Windows	MS16-153	goo.gl/xagnPS	2016-12-13	متوسط	آسیب‌پذیری آشکارسازی اطلاعات در ویندوز به واسطه‌ی نقص در مدیریت اشیاء در حافظه توسط راه‌انداز Windows Common Log File System در صورت اجرای یک برنامه‌ی کاربردی جعلی توسط مهاجم محلی برای دور زدن محدودیت‌های امنیتی	برای ویندوز 32-64bit SP1 7 : goo.gl/al0EM8 goo.gl/daEnO9 برای ویندوز 2012 R2 Server : goo.gl/qz71C7 goo.gl/uXS0oR برای ویندوز 32-64bit 10 1607 و Server 2016 64bit : goo.gl/s4G9sF	goo.gl/IpkH1M
Windows	MS16-152	goo.gl/HgTKzN	2016-12-13	متوسط	آسیب‌پذیری آشکارسازی اطلاعات در ویندوز به واسطه‌ی نقص در مدیریت اشیاء در حافظه توسط هسته‌ی ویندوز	برای ویندوز 32-64bit 10 1511 : goo.gl/9LkpGI برای ویندوز 32-64bit 10 1607 و Server 2016 64bit (GUI, : Core Installation) goo.gl/s4G9sF	goo.gl/rYHrdt
Windows	MS16-151	goo.gl/1VI60F	2016-12-13	متوسط	چندین آسیب‌پذیری افزایش سطح دسترسی در ویندوز به واسطه‌ی نقص در عملکرد Windows Secure Kernel Mode Driver در صورت اجرای یک برنامه‌ی کاربردی جعلی توسط مهاجم وارد شده به سیستم	برای ویندوز 32-64bit SP1 7 : goo.gl/al0EM8 goo.gl/daEnO9 برای ویندوز 32-64bit 10 1607 و Server 2016 64bit : goo.gl/s4G9sF	goo.gl/PhssPO goo.gl/U0nLib

goo.gl/O4xfCN	برای ویندوز 32-64bit 10 1511 : goo.gl/9LkpGI برای ویندوز 32-64bit 10 1607 و Server 2016 64bit (GUI, : Core Installation) goo.gl/s4G9sF	آسیب پذیری افزایش سطح دسترسی در ویندوز و نقض VTL به واسطه‌ی نقص در عملکرد Windows Secure Kernel Mode در صورت اجرای یک برنامه‌ی کاربردی جعلی توسط مهاجم احراز هویت شده	متوسط	2016-12-13	goo.gl/LvElA5	MS16-150	Windows
goo.gl/V1NVEV goo.gl/ujHcfh	برای ویندوز 32-64bit SP1 7 و : Server 2008 R2 64bit goo.gl/al0EM8 goo.gl/daEnO9 برای ویندوز 32-64bit 10 1607 و : Server 2016 64bit goo.gl/s4G9sF	چندین آسیب پذیری افزایش سطح دسترسی در ویندوز در صورت اجرای یک برنامه‌ی کاربردی جعلی توسط مهاجم احراز هویت شده	متوسط	2016-12-13	goo.gl/woQb66	MS16-149	Windows
goo.gl/UpKLmP	برای ویندوز 32-64bit R2 2012 : goo.gl/qz71C7 goo.gl/uXSOoR برای ویندوز 32-64bit 10 1607 و : Server 2016 64bit goo.gl/s4G9sF	آسیب پذیری اجرای کد از راه دور در ویندوز به واسطه‌ی عدم مدیریت صحیح اشیاء در حافظه توسط Windows Uniscribe در صورت مشاهده‌ی یک وبسایت جعلی و یا باز کردن یک داکيومنت جعلی	زیاد	2016-12-13	goo.gl/p6indt	MS16-147	Windows
goo.gl/E5NRdt goo.gl/H73xhI goo.gl/v643KH	برای ویندوز 32-64bit SP1 7 : goo.gl/al0EM8 goo.gl/daEnO9 برای ویندوز 32-64bit R2 2012 : goo.gl/qz71C7 goo.gl/uXSOoR برای ویندوز 32-64bit 10 1607 و : Server 2016 64bit goo.gl/s4G9sF	چندین آسیب پذیری اجرای کد از راه دور در ویندوز به واسطه‌ی عدم مدیریت صحیح اشیاء در حافظه توسط کامپوننت GDI در صورت مشاهده‌ی یک وبسایت جعلی و یا باز کردن یک داکيومنت جعلی	زیاد	2016-12-13	goo.gl/ZATWyX	MS16-146	Windows
goo.gl/jgeSc2 goo.gl/4OhDbm goo.gl/tfih49 ، ... goo.gl/8ReYb	برخی از آسیب پذیری‌ها در نسخه‌های بالا تر رفع گردیده و برای برخی هنوز راه حلی ارائه نشده است. goo.gl/8ReYb	چندین آسیب پذیری افزایش سطح دسترسی و جلبگیری از سرویس در نسخه‌های مختلف هسته‌ی لینوکس	زیاد	2016-12-08	goo.gl/AqhnLw goo.gl/FoTF2D goo.gl/QGfpNm ، ...	CVE-2016-9120 CVE-2016-8967 CVE-2016-8966 ، ...	Linux

goo.gl/Sf24nU goo.gl/vkFS3h goo.gl/wi6qzZ ، ...	آسیب پذیری های فوق در Android نسخه های 2016-11-01، 7.0، 6.x، 5.1.1، 5.0.2 و 4.4.4 برطرف گردیده است.	چندین آسیب پذیری افزایش سطح دسترسی، دسترسی به اطلاعات حساس، خرابی حافظه و جلوگیری از سرویس در Android	متوسط	2016-11-17	goo.gl/vNNDmg	CVE-2016-6722 CVE-2016-6720 CVE-2016-6712 ، ...	Android
goo.gl/1AP9sf	آسیب پذیری فوق در Debian Jessie در nginx نسخه 1.6.2-5+deb8u3 و در Ubuntu 16.10 در nginx نسخه 1.10.1-0ubuntu1.1 برطرف گردیده است. goo.gl/6xvMwD goo.gl/6gRMPl	آسیب پذیری افزایش سطح دسترسی در بسته های nginx در سیستم های عامل Debian و Ubuntu در صورت دسترسی کاربر محلی به حساب کاربری سرویس دهنده وب با استفاده از یک Symlink attack روی فایل ثبت خطا	زیاد	2016-10-25	goo.gl/QqTxgB	CVE-2016-1247	Debian, Ubuntu

محیط های برنامه نویسی

دریافت آخرین نسخه پایدار

لینک دریافت	تاریخ عرضه	آخرین نسخه پایدار	موضوع
goo.gl/ZEG0Nh	2016-12-13	3.6.5	Joomla!
goo.gl/c5F8At	2016-12-07	8.2.4	Drupal
goo.gl/DK0Wx	2016-12-06	4.7	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
-------	-------	------	--------------	---------	------------------------	----------	---------------

goo.gl/wcB7GN goo.gl/8q9LiR goo.gl/G1d3BZ	آسیب پذیری های فوق در Joomla نسخه 3.6.5 برطرف گردیده است. goo.gl/ZEG0Nh	چندین آسیب پذیری آشکار سازی اطلاعات حساس، افزایش سطح دسترسی و اجرای کد دلخواه در Joomla نسخه های ماقبل 3.6.5	زیاد	2016-12-13	goo.gl/YVOFAz	CVE-2016-9838 CVE-2016-9837 CVE-2016-9836	Joomla
goo.gl/R79a2T	برای .NET Framework نسخه 4.6.2 روی : ویندوز SP1 32-64bit و Server 2008 R2 64bit goo.gl/kb17S3 ویندوز 10 32-64bit و Server 2016 64bit goo.gl/s4G9sF	آسیب پذیری دسترسی به اطلاعات حساس در .NET Framework Data Provider نسخه 4.6.2 و در نهایت دسترسی مهاجم به اطلاعات محافظت شده با ویژگی Always Encrypted توسط SQL Sever	متوسط	2016-12-13	goo.gl/WjlQ7G	MS16-155	.NET Framework
goo.gl/jlT4zm goo.gl/32dZ6t goo.gl/qMB7qP goo.gl/IWwA9M	آسیب پذیری های فوق در Drupal نسخه های 8.2.3 و 7.52 برطرف گردیده است. goo.gl/c5F8At	چندین آسیب پذیری تزریق URL، جلوگیری از سرویس، به دست آوردن اطلاعات حساس و تغییرات در حافظه ی نهان در Drupal	زیاد	2016-11-16	goo.gl/dBIfsy	CVE-2016-9452 CVE-2016-9451 CVE-2016-9450 CVE-2016-9449	Drupal
goo.gl/2me1JJ goo.gl/RBSZYA	آسیب پذیری های فوق در Joomla نسخه 3.6.4 برطرف گردیده است. goo.gl/ZEG0Nh	آسیب پذیری های افزایش سطح دسترسی و ایجاد اکانت کاربری در Joomla نسخه های مابین 3.4.4 الی 3.6.3 به واسطه ی نقص در عملکرد فایل user.php	زیاد	2016-10-25	goo.gl/Vimztl goo.gl/hh5lZJ	CVE-2016-8870 CVE-2016-8869	Joomla
goo.gl/gG5jUV goo.gl/kaERCs goo.gl/sVJM0C	آسیب پذیری های فوق در Drupal نسخه 8.1.10 برطرف گردیده است. goo.gl/c5F8At	آسیب پذیری های دور زدن محدودیت های امنیتی، XSS و افزایش سطح دسترسی در Drupal نسخه های 8.x الی ماقبل 8.1.10	زیاد	2016-09-21	goo.gl/nfPGHS	CVE-2016-7572 CVE-2016-7571 CVE-2016-7570	Drupal

مرورگرهای اینترنت

دریافت آخرین نسخه ی پایدار

موضوع	آخرین نسخه پایدار	تاریخ عرضه	لینک دریافت
Mozilla Firefox	50.1.0	2016-12-13	goo.gl/yIXtW
Google Chrome	55.0.2883.87	2016-12-09	goo.gl/Jk2diZ

آسیب پذیری ها

موضوع	شناسه	منبع	تاریخ انتشار	سطح خطر	خلاصه ای از آسیب پذیری	نحوه رفع	اطلاعات بیشتر
Google Chrome	CVE-2016-5193 CVE-2016-5192 CVE-2016-5191 , ...	goo.gl/MuoumP goo.gl/2I7kdk goo.gl/1SJBX6 , ...	2016-12-17	زیاد	چندین آسیب پذیری دور زدن محدودیت های امنیتی، XSS، خواندن حافظه و غیره در مرورگر Google Chrome	آسیب پذیری های فوق در مرورگر Google Chrome نسخه 54.0 روی OS، نسخه 54.0.2840.85 روی اندروید و نسخه 54.0.2840.59 روی ویندوز، مک و لینوکس برطرف گردیده است.	goo.gl/V3OuAn goo.gl/eC7zqX goo.gl/NNNQJ9 , ...
Microsoft Edge	MS16-145	goo.gl/10XfJV	2016-12-13	زیاد	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	برای ویندوز 32-64bit : goo.gl/nV8AFb برای ویندوز 32-64bit : goo.gl/9LkpGI برای ویندوز 32-64bit : Server 2016 64bit goo.gl/s4G9sF	goo.gl/10XfJV
Internet Explorer	MS16-144	goo.gl/A5uYJv	2016-12-13	زیاد	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	برای مرورگر Internet Explorer نسخه 11 روی : ویندوز 32-64bit SP1 7 و Server 2008 R2 SP1 64bit goo.gl/al0EM8 goo.gl/daEnO9 ویندوز 32-64bit 10 1607 و Server 2016 64bit goo.gl/s4G9sF	goo.gl/A5uYJv

مجازی سازی

دریافت آخرین نسخه ی پایدار

موضوع	آخرین نسخه پایدار	تاریخ عرضه	لینک دریافت
VirtualBox	5.1.10	2016-11-21	goo.gl/l3wrf

آسیب پذیری ها

موضوع	شناسه	منبع	تاریخ انتشار	سطح خطر	خلاصه ای از آسیب پذیری	نحوه رفع	اطلاعات بیشتر
QEMU	CVE-2016-8910 CVE-2016-8909 CVE-2016-8669 ، ...	goo.gl/7nTzyN goo.gl/oAXdY4 goo.gl/KdNxtV ، ...	2016-11-04	متوسط	چندین آسیب پذیری جلوگیری از سرویس در QEMU به واسطه ی خطا در عملکرد توابع v9fs_iov_vunmarshal rc4030_write و rtl8139_cplus_transmit و غیره	تاکنون برای رفع آسیب پذیری های فوق راه حلی ارائه نگردیده است.	goo.gl/gsZuOc goo.gl/4yUygJ goo.gl/34uGl2 ، ...
Xen	CVE-2016-7154 CVE-2016-7094 CVE-2016-7093 CVE-2016-7092	goo.gl/ILwzoP goo.gl/V0jac9 goo.gl/q4ePQS goo.gl/Xwt6uN	2016-09-08	زیاد	چندین آسیب پذیری اجرای کد دلخواه، افزایش سطح دسترسی و جلوگیری از سرویس در Xen	وصله برای نسخه های 4.7.x : goo.gl/B9sTcn goo.gl/taQ3pT goo.gl/4i3Tdk سایر وصله ها در لینک های زیر : goo.gl/ILwzoP goo.gl/V0jac9 goo.gl/q4ePQS goo.gl/Xwt6uN	goo.gl/Gm7kJr goo.gl/7lic6T goo.gl/zdZ5hj goo.gl/MjP4DO
VMware vCenter	CVE-2016-5331	goo.gl/SfJM3c	2016-08-04	متوسط	آسیب پذیری تزریق سرآیند HTTP دلخواه در VMware vCenter Server و ESXi	آسیب پذیری فوق در VMware vCenter Server نسخه ی 6.0 U2 برطرف گردیده است.	goo.gl/X4xoKm

تجهیزات شبکه، دیوارهای آتش و ضدبدافزار

موضوع	شناسه	منبع	تاریخ انتشار	سطح خطر	خلاصه‌ای از آسیب پذیری	نحوه رفع	اطلاعات بیشتر
Cisco ASR	CVE-2016-9203	goo.gl/P1DIJjA	2016-12-07	متوسط	آسیب پذیری توقف پردازش ipsecmgr و نیاز به برپایی مجدد اتصال در مسیرهای Cisco ASR سری 5000 با نسخه های نرم افزاری 20.2.3 و 20.2.3.65026 با استفاده از ارسال بسته های IKEv2 جعلی	آسیب پذیری فوق در Cisco ASR با نسخه های نرم افزاری 21.1.PP0.65733، 21.1.M0.65431 و غیره برطرف گردیده است.	goo.gl/DtmNpJ
Fortinet	CVE-2015-7363	goo.gl/CbV1zZ	2016-10-05	کم	آسیب پذیری تزریق اسکریپت وب دلخواه و یا HTML در صفحه ی تنظیمات پیشرفته FortiManager و FortiAnalyzer به واسطه ی وجود XSS در فیلد add filter	آسیب پذیری فوق در FortiManager نسخه های 5.0.12، 5.2.3 و 5.4.0 و در FortiAnalyzer نسخه های 5.0.13، 5.2.3 و 5.4.0 برطرف گردیده است.	goo.gl/wLVVvC
Sophos UTM	CVE-2016-7442 CVE-2016-7397	goo.gl/zCOi7x goo.gl/dTm8To	2016-10-04	متوسط	آسیب پذیری به دست آوردن اطلاعات در Sophos UTM با نسخه های نرم افزاری 5-9.405 و ماقبل آن	تاکنون برای رفع آسیب پذیری فوق راه حلی ارائه نگردیده است.	goo.gl/OcfLaC goo.gl/WrKKbK
نرم افزارهای کاربردی							
موضوع	شناسه	منبع	تاریخ انتشار	سطح خطر	خلاصه‌ای از آسیب پذیری	نحوه رفع	اطلاعات بیشتر

goo.gl/o9w5n6 goo.gl/A3L5FB goo.gl/0VU0LK ...	این آسیب‌پذیری‌ها در Adobe Flash Player 24.0.0.186 در ویندوز و مک و لینوکس برطرف گردیده است. goo.gl/qDW9E مرورگرهای Internet Explorer و Microsoft Edge و Google Chrome را به‌روزرسانی کنید. ویندوزهای 8.1 و 10 را به‌روزرسانی نمائید.	چندین آسیب‌پذیری اجرای کد دلخواه، دور زدن محدودیت‌های امنیتی، Use after free، سرریزی بافر و غیره در Adobe Flash Player در سیستم‌های عامل ویندوز، لینوکس و مک	زیاد	2016-12-14	goo.gl/rgJn80	APSB16-39	Adobe Flash Player
goo.gl/kyOtfD goo.gl/LXJjMr goo.gl/iEobZp	از آخرین نسخه‌ی درایورهای گرافیک NVIDIA استفاده نمائید. goo.gl/LGhxO	چندین آسیب‌پذیری سرریزی بافر، جلوگیری از سرویس، دسترسی به حافظه‌ی فیزیکی و غیره در درایورهای گرافیک NVIDIA	زیاد	2016-12-14	goo.gl/NbjdE6 goo.gl/C2d8zj goo.gl/wIyMJt	CVE-2016-8827 CVE-2016-8826 CVE-2016-8825	NVIDIA
goo.gl/cSUaJ9	تاکنون راه حلی برای رفع آسیب‌پذیری فوق ارائه نگردیده است.	آسیب‌پذیری پیمایش دایرکتوری در GNU tar نسخه‌های مابین 1.14 الی 1.29 به علت نقص در پاک‌سازی اطلاعات ورودی به واسطه‌ی نقص در عملکرد تابع safer_name_suffix	زیاد	2016-12-14	goo.gl/yyFc5D	CVE-2016-6321	GNU tar
goo.gl/rtq217	برای Office 2013 32bit : goo.gl/DIw4Qi goo.gl/FQ7Tsv برای Office 2011 روی مک : goo.gl/juMAS6	چندین آسیب‌پذیری اجرای کد از راه دور در Microsoft Office در صورت باز کردن یک فایل Office جعلی در ویندوز و مک	زیاد	2016-12-13	goo.gl/rtq217	MS16-148	Microsoft Office
goo.gl/F985B2	آسیب‌پذیری‌های فوق در WinCC نسخه‌های 7.2 به بعد و PCS 7 نسخه‌های SP1 8.0 به بعد برطرف گردیده است.	آسیب‌پذیری‌های توقف ناگهانی یک کامپوننت ActiveX و خطای حافظه در نرم‌افزارهای کنترل سیستم‌های صنعتی Siemens در صورت کلیک کردن کاربر روی یک لینک مخرب	----	2016-12-16	goo.gl/LrgfUB	CVE-2016-9160	WinCC, PCS
goo.gl/9TI9Ne	تاکنون راه حلی برای رفع آسیب‌پذیری فوق ارائه نگردیده است.	آسیب‌پذیری جلوگیری از سرویس در OpenSSH نسخه‌های 6.x الی 7.3 به واسطه‌ی نقص در عملکرد تابع kex_input_kexinit با ارسال چندین درخواست KEXINIT	زیاد	2016-12-09	goo.gl/mnMWeF	CVE-2016-8858	OpenSSH

goo.gl/q22sgL	آسیب‌پذیری فوق در نسخه‌ی 18.1.1607.3129 برطرف گردیده است. goo.gl/9vY0mg	آسیب‌پذیری Unquoted service path در درایورهای Intel Wireless Bluetooth نسخه‌های 16.x الی ماقبل 18.1.1607.3129	زیاد	2016-12-06	goo.gl/iOEqEZ	CVE-2016-8102	Intel Wireless Bluetooth Driver
goo.gl/FJ911Y goo.gl/cw2oDY goo.gl/QtWNI4 , ...	آسیب‌پذیری‌های فوق در phpMyAdmin نسخه‌های 4.6.5، 4.0.10.18 و 4.4.15.9 برطرف گردیده است. goo.gl/j3gQ4B	چندین آسیب‌پذیری CSRF، تزریق SQL، دور زدن محدودیت‌های امنیتی، تزریق BBCode، دور زدن محدودیت فهرست سفید، جلوگیری از سرویس و غیره در phpMyAdmin	زیاد	2016-11-25	goo.gl/cs74ps goo.gl/w5xRw9 goo.gl/xt2U69 , ...	CVE-2016-9866 CVE-2016-9865 CVE-2016-9864 , ...	phpMyAdmin
goo.gl/YqQlk4 goo.gl/bsZxAs goo.gl/oDbxcG , ...	تاکتون راه حلی برای رفع آسیب‌پذیری فوق ارائه نگردیده است.	چندین آسیب‌پذیری سرریزی مقدار عدد صحیح، سرریزی بافر و غیره در libtiff نسخه‌ی 4.0.6	زیاد	2016-11-22	goo.gl/gLVkjo goo.gl/jJHRrw goo.gl/bocmC7 , ...	CVE-2016-9540 CVE-2016-9539 CVE-2016-9538 , ...	libtiff
goo.gl/nKdtmX goo.gl/ksfo8i goo.gl/A4Yffc , ...	آسیب‌پذیری‌های فوق در Wireshark نسخه‌های 2.2.2 و بالاتر از آن برطرف گردیده است. goo.gl/gY4xk	چندین آسیب‌پذیری جلوگیری از سرویس در Wireshark با تزریق یک بسته‌ی تغییرشکل یافته و یا ترغیب قربانی به خواندن یک فایل pcap جعلی	متوسط	2016-11-16	goo.gl/SCsPds goo.gl/bCkp2k goo.gl/UZKZlu , ...	CVE-2016-9376 CVE-2016-9375 CVE-2016-9374 , ...	Wireshark
goo.gl/Awz7PZ goo.gl/NOvPhZ goo.gl/Tq1q2C , ...	آسیب‌پذیری‌های فوق در X.org نسخه‌ی 1.16.4 و در کتابخانه‌ی libXvMC نسخه‌ی 1.0.10، کتابخانه‌ی libXtst نسخه‌ی 1.2.3 و غیره برطرف گردیده است.	آسیب‌پذیری جلوگیری از سرویس در X.org نسخه‌های ماقبل 1.16.4 و چندین آسیب‌پذیری افزایش سطح دسترسی، جلوگیری از سرویس و غیره در کتابخانه‌های libXtst، libXvMC، libXrender و غیره	زیاد	2016-10-04	goo.gl/6uTuJm goo.gl/8Gd8pA	CVE-2016-7953 CVE-2016-7952 CVE-2016-7951 , ...	X.org
goo.gl/X4LQOZ	آسیب‌پذیری‌های فوق در نسخه‌های 15.33.43.4425، 15.33.43.4425، 15.36.31.64.4414 و 15.40.25.4463 برطرف گردیده است. goo.gl/ArIjNi	آسیب‌پذیری‌های افزایش سطح دسترسی و جلوگیری از سرویس در درایورهای Intel Graphic به واسطه‌ی نقص در عملکرد ماژول igdkmd64	----	2016-08-31	goo.gl/0dTjdM	CVE-2016-5647	Intel Graphics Driver

goo.gl/rGJYGr goo.gl/wPKD9C	آسیب‌پذیری‌های فوق در PostgreSQL نسخه‌های 9.5.4, 9.1.23 و 9.2.18, 9.3.14, 9.4.9 برطرف گردیده است. goo.gl/bBkHkd	چندین آسیب‌پذیری افزایش سطح دسترسی و اجرای کد دلخواه، به دست آوردن اطلاعات حساس و جلوگیری از سرویس در PostgreSQL	زیاد	2016-08-11	goo.gl/WR1i8p	CVE-2016-5424 CVE-2016-5423	PostgreSQL
goo.gl/zYUCsq goo.gl/WG3Ra4	آسیب‌پذیری‌های فوق در 7-Zip نسخه‌ی 16.00 برطرف گردیده است. goo.gl/13O4	آسیب‌پذیری‌های اجرای کد دلخواه و جلوگیری از سرویس در 7-Zip به واسطه‌ی بروز خطا در خواندن حافظه و همچنین سرریزی بافر مبتنی بر هیپ	زیاد	2016-05-12	goo.gl/SnjbHq	CVE-2016-2335 CVE-2016-2334	7-Zip
goo.gl/8nOcts goo.gl/yoot5e goo.gl/LDBcDC , ...	تاکنون راه حلی برای رفع آسیب‌پذیری فوق ارائه نگردیده است.	چندین آسیب‌پذیری سرریزی بافر مبتنی بر هیپ و جلوگیری از سرویس در OpenJPEG نسخه‌ی 2.1.2	متوسط	2016-10-30	goo.gl/hY1axS goo.gl/J53Ug4 goo.gl/BgMu4Q , ...	CVE-2016-9118 CVE-2016-9117 CVE-2016-9116 , ...	OpenJPEG
goo.gl/xW84o2 goo.gl/LWdo4V goo.gl/yrqbqj , ...	آسیب‌پذیری فوق در Acrobat DC و Acrobat Reader DC و نسخه‌های Continuous و Classic به ترتیب در نسخه‌های 15.006.30243 و 15.020.20039 Reader XI و Acrobat XI در نسخه‌ی 11.0.18 برطرف گردیده است. goo.gl/9E1Y6	چندین آسیب‌پذیری جلوگیری از سرویس در Acrobat DC و Acrobat Reader DC نسخه‌های Continuous و Classic و در Acrobat XI Reader XI	زیاد	2016-10-21	goo.gl/qpcBeo	APSB16-33	Adobe Acrobat, Reader