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	2.4.23	2016-07-05	goo.gl/ySdR
Squid Proxy & Cache Server	3.5.22	2016-10-09	goo.gl/ZCyZ6f

آسیب‌پذیری‌ها

موضوع	شناسه	منبع	تاریخ انتشار	سطح خطر	خلاصه‌ای از آسیب‌پذیری	نحوه رفع	اطلاعات بیشتر
Microsoft SQL Server	MS16-136	goo.gl/27XbVU	2016-11-08	متوسط	چندین آسیب‌پذیری افزایش سطح دسترسی و به دست آوردن توانایی مشاهده، تغییرات و یا پاک کردن داده‌ها 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	آسیب‌پذیری جلوگیری از سرویس در ISC BIND به واسطه‌ی نقص در عملکرد db.c و resolver.c با استفاده از یک رکورد DNAME در بخش answer یک پاسخ جستجوی بازگشتی	آسیب‌پذیری فوق در ISC BIND نسخه‌های 9.9.9-P4، 9.10.4-P4 و 9.11.0-P1 برطرف گردیده است. goo.gl/E3i9do	goo.gl/QJdi5r

Microsoft Exchange Server	MS16-108	goo.gl/YhhEv2	2016-09-13	زیاد	چندین آسیب‌پذیری اجرای کد از راه دور در Microsoft Exchange Server با استفاده از ارسال یک ایمیل دارای پیوست جعلی به یک سرویس‌دهنده‌ی آسیب‌پذیر	برای Microsoft Exchange Server 2010 SP3 : goo.gl/Wk7EU5 برای Microsoft Exchange Server 2016 CU1, CU2 : CU1: goo.gl/Zv8r48 CU2: goo.gl/o5UliO	goo.gl/LxExNR goo.gl/CxmK4y goo.gl/gH5Udz
سیستم‌های عامل							
موضوع	**شناسه**	**منبع**	**تاریخ انتشار**	**سطح خطر**	**خلاصه‌ای از آسیب‌پذیری**	**نحوه رفع**	**اطلاعات بیشتر**
Windows	MS16-141	goo.gl/GzgidI	2016-11-08	زیاد	چندین آسیب‌پذیری در Adobe Flash Player در ویندوز	برای ویندوز نسخه‌های 8.1 32, 64bit، Server 2012، Server 2012 R2، RT 8.1، 10 و Server 2016 : goo.gl/ZePWcT	goo.gl/GzgidI
Windows	MS16-140	goo.gl/qxOEcT	2016-11-08	متوسط	آسیب‌پذیری دور زدن محدودیت‌های امنیتی سازوکار Secure Boot در ویندوز در صورت نصب یک سیاست بوت جعلی	برای ویندوز 8.1 32, 64bit و ویندوز Server 2012 R2 : goo.gl/YZCjzN goo.gl/l9MYei برای ویندوز 10 و ویندوز Server 2016 64bit : KB3198585 KB3198586 KB3200970	goo.gl/gUikJK
Windows	MS16-139	goo.gl/v8582d	2016-11-08	متوسط	آسیب‌پذیری افزایش سطح دسترسی در ویندوز به واسطه‌ی نقص در عملکرد هسته‌ی ویندوز در صورت اجرای یک برنامه‌ی کاربردی جعلی توسط مهاجم محلی جهت دسترسی به اطلاعات حساس	برای ویندوز 7 32, 64bit : goo.gl/zV8HNa goo.gl/gdZAlt	goo.gl/jkbYB6

Windows	MS16-138	goo.gl/g2zhjj	2016-11-08	متوسط	چندین آسیب‌پذیری افزایش سطح دسترسی در ویندوز به واسطه‌ی نقص در مدیریت دسترسی به فایل‌هـا در درایور VHD	برای ویندوز 8.1 32, 64bit و ویندوز Server 2012 R2 : goo.gl/YZCjzN goo.gl/l9MYei برای ویندوز 10 و ویندوز Server 2016 64bit : KB3198585 KB3198586 KB3200970	goo.gl/dQHwX7 goo.gl/rKsofr goo.gl/GLy3JP goo.gl/41GKfy
Windows	MS16-137	goo.gl/I61Lr7	2016-11-08	متوسط	چندین آسیب‌پذیری افزایش سطح دسترسی در ویندوز پس از ورود مهاجم به سیستم قربانی تحت دومین بـا استفاده از یک گـواهی‌نامـه‌ی معتبـر و اجـرای یـک برنامه‌ی کاربردی جعلی طراحی شده برای دسـتکاری درخواست تغییر کلمه‌ی عبور NTLM	برای ویندوز 7 32, 64bit : goo.gl/zV8HNa goo.gl/gdZAlt بـرای ویننـدوز 8.1 32, 64bit و ویندوز Server 2012 R2 : goo.gl/YZCjzN goo.gl/l9MYei ویندوز 10 را به‌روزرسانی نمائید. KB3198585 KB3198586 KB3200970	goo.gl/JWMf8E goo.gl/fkP3n4 goo.gl/TVenSh
Windows	MS16-135	goo.gl/wx699C	2016-11-08	متوسط	چندین آسیب‌پذیری افزایش سطح دسترسی در ویندوز در صورت ورود مهاجم به سیستم قربانی و اجرای یک برنامه‌ی کاربردی جعلی	برای ویندوز 7 32, 64bit : goo.gl/zV8HNa goo.gl/gdZAlt بـرای ویننـدوز 8.1 32, 64bit و ویندوز Server 2012 R2 : goo.gl/YZCjzN goo.gl/l9MYei ویندوز 10 را به‌روزرسانی نمائید. KB3198585 KB3198586 KB3200970	goo.gl/wx699C

Windows	MS16-134	goo.gl/998asM	2016-11-08	متوسط	چندین آسیب‌پذیری افزایش سطح دسترسی در ویندوز با اجرای یک برنامه‌ی کاربردی جعلی روی سیستم قربانی به واسطه‌ی مدیریت ناصحیح اشیاء در حافظه توسط درایور CLFS	برای ویندوز 8.1 32, 64bit و ویندوز Server 2012 R2 : goo.gl/YZCjzN goo.gl/l9MYei برای ویندوز 10 و ویندوز Server 2016 64bit : goo.gl/I2SXOH goo.gl/9vBM2R goo.gl/8wR9Nd	goo.gl/998asM
Windows	MS16-132	goo.gl/xK2HZd	2016-11-08	زیاد	چندین آسیب‌پذیری اجرای کد از راه دور در ویندوز به واسطه‌ی مدیریت ناصحیح کتابخانه‌ی فونت ویندوز روی فونت‌های اضافه شده‌ی جعلی	برای ویندوز 7 32, 64bit : goo.gl/zV8Hna برای ویندوز 8.1 32, 64bit و ویندوز Server 2012 R2 : goo.gl/YZCjzN goo.gl/l9MYei برای ویندوز 10 : goo.gl/I2SXOH goo.gl/9vBM2R goo.gl/8wR9Nd	goo.gl/SA04y6 goo.gl/gmFZdJ goo.gl/N8MZvQ goo.gl/TPJUZB
Windows	MS16-131	goo.gl/OKvKbw	2016-11-08	زیاد	آسیب‌پذیری اجرای کد از راه دور در ویندوز به واسطه‌ی عدم مدیریت مناسب اشیاء در حافظه توسط Video Control با ترغیب قربانی به باز کردن یک فایل یا برنامه یا وب‌سایت مخرب	برای ویندوز 8.1 32, 64bit و ویندوز Server 2012 R2 : goo.gl/l9MYei ویندوز 10 را به‌روزرسانی نمائید. KB3198585 KB3198586 KB3200970	goo.gl/87YzkE
Windows	MS16-130	goo.gl/VA1Fze	2016-11-08	زیاد	چندین آسیب‌پذیری اجرای کد از راه دور در ویندوز در صورت اجرای یک برنامه‌ی کاربردی جعلی توسط مهاجم احراز هویت شده روی سیستم	برای ویندوز 8.1 32bit و ویندوز Server 2012 R2 : goo.gl/l9MYei ویندوز 10 را به‌روزرسانی نمائید. KB3198585 KB3198586 KB3200970	goo.gl/3pIVUc goo.gl/ruovy3 goo.gl/lOZTRE

Linux	CVE-2016-8666 CVE-2016-8660 CVE-2016-8658 , …	goo.gl/bmRDZU goo.gl/cpxEbh goo.gl/HlKJco , …	2016-10-18	متوسط	چندین آسیب‌پذیری افزایش سطح دسترسی، جلوگیری از سرویس، اجرای کد از راه دور و غیره در نسخه‌های مختلف هسته‌ی لینوکس	برخی از آسیب‌پذیری‌ها در نسخه‌های بالاتر رفع گردیده و برای برخی هنوز راه حلی ارائه نشده است. goo.gl/8ReYb	goo.gl/z2qBuw goo.gl/9M9oUo goo.gl/AiSiuw , …
Windows	MS16-128	goo.gl/PPlRIe	2016-10-27	زیاد	چندین آسیب‌پذیری در Adobe Flash Player در ویندوز	برای ویندوز 8.1 32bit : goo.gl/308qjU برای ویندوز Server 2012 R2 : goo.gl/1OwWS4 ویندوز 10 را به‌روزرسانی نمائید. KB3201860	goo.gl/PPlRIe
Windows	MS16-127	goo.gl/kvzEUE	2016-10-11	زیاد	چندین آسیب‌پذیری در Adobe Flash Player در ویندوز	برای ویندوز 8.1 64bit : goo.gl/44eW7o برای ویندوز Server 2012 R2 : goo.gl/gkp0ax ویندوز 10 را به‌روزرسانی نمائید. KB3194343	goo.gl/kvzEUE
Windows	MS16-126	goo.gl/P7xowY	2016-10-11	کم	آسیب‌پذیری آشکارسازی اطلاعات در ویندوز به واسطه‌ی مدیریت نامناسب اشیاء در حافظه توسط Microsoft Internet Messaging API و سوءاستفاده مهاجم از آن جهت کسب اطمینان از وجود یک فایل روی هارد سیستم	برای ویندوز 7 SP1 32bit : goo.gl/71x2rJ goo.gl/6wQqfM برای ویندوز Server 2008 R2 SP1 64bit : goo.gl/CvJhKf goo.gl/5KcGzZ	goo.gl/0V9CAv
Windows	MS16-125	goo.gl/xsg7jU	2016-10-11	متوسط	آسیب‌پذیری افزایش سطح دسترسی در ویندوز به واسطه‌ی عدم پاکسازی ورودی توسط سرویس Diagnostics Hub Standard Collector در صورت ورود مهاجم به سیستم قربانی و اجرای یک برنامه‌ی کاربردی جعلی	ویندوز 10 را به‌روزرسانی نمائید. KB3192440 KB3192441 KB3194798	goo.gl/d1nelr

Windows	MS16-124	goo.gl/m6RctZ	2016-10-11	متوسط	چندین آسیب‌پذیری افزایش سطح دسترسی در ویندوز در صورت دسترسی مهاجم بـه اطلاعـات رجیسـتری حساس	برای ویندوز 7 SP1 64bit : goo.gl/AYPRln goo.gl/CnjxSd ویندوز 10 را به‌روزرسانی نمائید. KB3192440 KB3192441 KB3194798	goo.gl/m6RctZ
Windows	MS16-123	goo.gl/fjw9Ri	2016-10-11	متوسط	چندین آسیب‌پذیری افزایش سطح دسترسی در ویندوز در صورت ورود مهاجم به سیستم قربانی و اجرای یک برنامه‌ی کاربردی جعلی	برای ویندوز 8.1 32bit : goo.gl/CUXnGh goo.gl/wjmQb0 برای ویندوز Server 2012 R2 : goo.gl/9dq8Rx ویندوز 10 را به‌روزرسانی نمائید. KB3192440 KB3192441 KB3194798	goo.gl/fjw9Ri
Windows	MS16-122	goo.gl/cqd1eh	2016-10-11	زیاد	آسـیب‌پـذیری اجـرای کـد از راه دور در ویـنـدوز بـه واسطه‌ی عدم مدیریت مناسب اشیاء در حافظه توسط Video Control	برای ویندوز 7 SP1 32bit : goo.gl/71x2rJ goo.gl/6wQqfM برای ویندوز 7 SP1 64bit : goo.gl/AYPRln goo.gl/CnjxSd ویندوز 10 را به‌روزرسانی نمائید. KB3192440 KB3192441 KB3194798	goo.gl/4N2ZcV
Windows	MS16-120	goo.gl/Xtwkep	2016-10-11	زیاد	چندین آسیب‌پذیری اجرای کد از راه دور در Office، Skype for Business، Silverlight و Lync سیسـتم عامـل ویـنـدوز در صـورت مشـاهده‌ی یـک وب‌سایت جعلی و یا باز کردن یک داکیومنت جعلی	برای ویندوز 7 SP1 32bit : goo.gl/71x2rJ goo.gl/6wQqfM برای ویندوز Server 2012 R2 : goo.gl/9dq8Rx goo.gl/UrtAVo ویندوز 10 را به‌روزرسانی نمائید. KB3192440 KB3192441 KB3194798	goo.gl/Xtwkep

موضوع	شناسه	منبع	تاریخ انتشار	سطح خطر	خلاصه‌ای از آسیب‌پذیری	نحوه رفع	اطلاعات بیشتر
Android	CVE-2016-6696 CVE-2016-6695 CVE-2016-6694 , ...	goo.gl/jDCVGd	2016-10-04	زیاد	چندین آسیب‌پذیری اجرای کد دلخواه، افزایش سطح دسترسی، آشکارسازی اطلاعات و جلوگیری از سرویس در Android	آسیب‌پذیری‌های فوق در Android نسخه‌ی 2016-10-05 برطرف گردیده است.	goo.gl/CR04Sb goo.gl/cZM2fR goo.gl/adG4rX , ...

محیط‌های برنامه‌نویسی

دریافت آخرین نسخه‌ی پایدار

موضوع	آخرین نسخه پایدار	تاریخ عرضه	لینک دریافت
Joomla!	**3.6.4**	**2016-10-25**	**goo.gl/ZEG0Nh**
Drupal	**8.2.2**	**2016-11-02**	**goo.gl/c5F8At**
WordPress	**4.6.1**	**2016-09-07**	**goo.gl/DK0Wx**
DotNetNuke	**8.00.03**	**2016-05-26**	**goo.gl/pT76iH**

آسیب‌پذیری‌ها

موضوع	شناسه	منبع	تاریخ انتشار	سطح خطر	خلاصه‌ای از آسیب‌پذیری	نحوه رفع	اطلاعات بیشتر
Joomla	CVE-2016-8870 CVE-2016-8869	goo.gl/Vimztl goo.gl/hh5lZJ	2016-10-25	زیاد	آسیب‌پذیری‌های افزایش سطح دسترسی و ایجاد اکانت کاربری در Joomla نسخه‌های مابین 3.4.4 الی 3.6.3 به واسطه‌ی نقص در عملکرد فایل user.php	آسیب‌پذیری‌های فوق در Joomla نسخه‌ی 3.6.4 برطرف گردیده است. goo.gl/ZEG0Nh	goo.gl/2me1JJ goo.gl/RBSZYA
Drupal	CVE-2016-7572 CVE-2016-7571 CVE-2016-7570	goo.gl/nfPGHS	2016-09-21	زیاد	آسیب‌پذیری‌های دور زدن محدودیت‌های امنیتی، XSS و افزایش سطح دسترسی در Drupal نسخه‌های 8.x الی ماقبل 8.1.10	آسیب‌پذیری‌های فوق در Drupal نسخه‌ی 8.1.10 برطرف گردیده است. goo.gl/c5F8At	goo.gl/gG5jUV goo.gl/kaERCs goo.gl/sVJM0C

PHP	CVE-2016-7418 CVE-2016-7417 CVE-2016-7416 , …	goo.gl/9YrzdW goo.gl/KrFSQ7 goo.gl/4HE73P , …	2016-09-12	زیاد	چندین آسیب‌پذیری جلوگیری از سرویس در PHP به واسطه‌ی نقص در عملکرد wddx.c، spl_array.c، msgformat_format.c و غیره	آسیب‌پذیری‌های فوق در PHP نسخه‌های 5.6.26 و 7.0.11 برطرف گردیده است. goo.gl/DGeo	goo.gl/rPpwM8 goo.gl/rzdbx6 goo.gl/k1Xi8w , …

مرورگرهای اینترنت

دریافت آخرین نسخه‌ی پایدار

موضوع	آخرین نسخه پایدار	تاریخ عرضه	لینک دریافت
Mozilla Firefox	**49.0.2**	**2016-10-20**	**goo.gl/yIXtW**
Google Chrome	**54.0.2840.99**	**2016-11-09**	**goo.gl/Jk2diZ**

آسیب‌پذیری‌ها

موضوع	شناسه	منبع	تاریخ انتشار	سطح خطر	خلاصه‌ای از آسیب‌پذیری	نحوه رفع	اطلاعات بیشتر
Internet Explorer	MS16-142	goo.gl/TaMkgZ	2016-11-08	زیاد	چندین آسیب‌پذیری اجرای کد از راه دور، افزایش سطح دسترسی، ایجاد تغییرات در فایل‌ها و غیره در Internet Explorer در صورت مشاهده‌ی یک صفحه‌ی وب جعلی	برای مرورگر Internet Explorer نسخه‌ی 11 روی ویندوز 7 SP1 32, 64bit : goo.gl/zV8HNa goo.gl/gdZAlt ویندوز 8.1 32, 64bit و ویندوز Server 2012 R2 : goo.gl/YZCjzN goo.gl/l9MYei	goo.gl/TaMkgZ
Microsoft Edge	MS16-129	goo.gl/7tM1or	2016-11-08	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. KB3198585 KB3198586 KB3200970	goo.gl/ENs0K1

Microsoft Edge	MS16-119	goo.gl/ENs0K1	2016-10-11	زیاد	چندین آسیب‌پذیری اجـرای کـد از راه دور و افـزایش سطح دسترسـی در مرورگـر Microsoft Edge در صورت مشاهده‌ی یک صفحه‌ی وب جعلی	ویندوز 10 را به‌روزرسانی نمائید. KB3192440 KB3192441 KB3194798	goo.gl/ENs0K1
Internet Explorer	MS16-118	goo.gl/7HGaik	2016-10-11	زیاد	چندین آسیب‌پـذیری اجـرای کـد از راه دور، افـزایش سطح دسترسی، ایجاد تغییرات در فایل‌هـا و غیـره در Internet Explorer در صـورت مشـاهده‌ی یـک صفحه‌ی وب جعلی	بـرای مرورگـر Internet Explorer نسـخه‌ی 10 روی ویـنـدوز Server 2012 R2 : goo.gl/bn2wHP goo.gl/jEIaZI ویندوز 10 را به‌روزرسانی نمائید. KB3192440 KB3192441 KB3194798	goo.gl/7HGaik
Google Chrome	CVE-2016-5176 CVE-2016-7549 CVE-2016-5175 , …	goo.gl/0e7Vbi goo.gl/BKlbrM goo.gl/1EfmEK , …	2016-09-29	زیاد	چندین آسیب‌پذیری آشکارسازی اطلاعـات حسـاس، دور زدن محدودیت‌های امنیتی، جلوگیری از سرویس، به دست آوردن اطلاعات حساس و غیـره در مرورگـر Google Chrome	آسـیب‌پـذیری‌هـای فـوق در مرورگـر Google Chrome نســـخه‌ی 53.0.2785.113 برطـرف گردیـده است. goo.gl/Jk2diZ	goo.gl/egUIMu goo.gl/Al5B1t goo.gl/fYfScy , …
Mozilla Firefox, ESR	CVE-2016-5284 CVE-2016-5283 CVE-2016-5282 , …	goo.gl/fMK2QM goo.gl/zY6JAs	2016-09-20	زیاد	چنـدین آسـیب‌پـذیری MitM، بـه دسـت آوردن اطلاعات حساس، سرریزی بافر مبتنی بـر هیـپ، دور زدن محدودیت‌هـای امنیتـی، اجـرای کـد از راه دور، جلوگیری از سرویس و غیـره در مرورگـر Mozilla Firefox و Firefox ESR	آسـیب‌پـذیری‌هـای فـوق در مرورگـر Mozilla Firefox نسـخه‌ی 49.0 و در Firefox ESR نسخه‌ی 45.4 برطرف گردیده است. goo.gl/yIXtW goo.gl/8WbxPl	goo.gl/NCUOCZ goo.gl/Qw8NEe goo.gl/WYn6Xb , …

مجازی‌سازی

دریافت آخرین نسخه‌ی پایدار

موضوع	آخرین نسخه پایدار	تاریخ عرضه	لینک دریافت
VirtualBox	**5.1.8**	**2016-10-18**	**goo.gl/l3wrf**

آسیب‌پذیری‌ها							
موضوع	شناسه	منبع	تاریخ انتشار	سطح خطر	خلاصه‌ای از آسیب‌پذیری	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 آسیب‌پذیری جلوگیری از سرویس در QEMU به واسطه‌ی خطا در عملکرد توابع rc4030_write، v9fs_iov_vunmarshal، rtl8139_cplus_transmit و غیره	تاکنون برای رفع آسیب‌پذیری‌های 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 آسیب‌پذیری اجرای کد دلخواه، افزایش سطح دسترسی و جلوگیری از سرویس در Xen	وصله برای نسخه‌های 4.7.x : goo.gl/B9sTcn goo.gl/taQ3pT goo.gl/4i3Tdk سایر وصله‌ها در لینک‌های زیر : goo.gl/ILwzoP goo.gl/V0jac9 goo.gl/q4ePQS goo.gl/Xwt6uN	goo.gl/Gm7kJr goo.gl/7Iic6T goo.gl/zdZ5hj goo.gl/MjP4DO
VMware vCenter	CVE-2016-5331	goo.gl/SfJM3c	2016-08-04	متوسط	آسیب‌پذیری تزریق سرآیند HTTP دلخواه در VMware vCenter Server و ESXi	آسیب‌پذیری فوق در VMware vCenter Server نسخه‌ی 6.0 U2 برطرف گردیده است.	goo.gl/X4xoKm

تجهیزات شبکه، دیواره‌های آتش و ضدبدافزار							
موضوع	شناسه	منبع	تاریخ انتشار	سطح خطر	خلاصه‌ای از آسیب‌پذیری	نحوه رفع	اطلاعات بیشتر
Cisco ASR	CVE-2016-6441	goo.gl/Ur1htX	2016-11-02	زیاد	آسیب‌پذیری بارگذاری مجدد و اجرای کد از راه دور در مسیریاب‌های Cisco ASR سری 900 به علت نقص در بررسی داده‌های ورودی با استفاده از ارسال یک درخواست مخرب به پورت TL1	آسیب‌پذیری فوق در Cisco IOS XE نسخه‌های 3.18.2S و 3.17.3S برطرف گردیده است.	goo.gl/UEkzl1

Fortinet	CVE-2015-7363	goo.gl/CbV1zZ	2016-10-05	کم	آسیب‌پذیری تزریق اسکریپت وب دلخواه و یا HTML در صفحه‌ی تنظیمات پیشرفته FortiManager و FortiAnalyzer به واسطه‌ی وجود XSS در فیلد add filter	آسیب‌پذیری فوق در FortiManager نسخه‌های 5.0.12، 5.2.3 و 5.4.0 و در FortiAnalyzer نسخه‌های 5.0.13، 5.2.3 و 5.4.0 برطرف گردیده است.	goo.gl/wLVVvC
Avast	CVE-2016-4025	goo.gl/ZAywFJ	2016-04-19	متوسط	آسیب‌پذیری دور زدن ویژگی DeepScreen در نسخه‌های مختلف Avast از جمله Internet Security، Free Antivirus، Pro Antivirus، Endpoint Protection Suite Plus و غیره با استفاده از فراخوانی DeviceIoControl	تاکنون برای رفع آسیب‌پذیری‌های فوق راه حلی ارائه نگردیده است.	goo.gl/TvpuR6
Sophos UTM	CVE-2016-7442 CVE-2016-7397	goo.gl/zCOi7x goo.gl/dTm8To	2016-10-04	متوسط	آسیب‌پذیری به دست آوردن اطلاعات در Sophos UTM با نسخه‌های نرم‌افزاری 5-9.405 و ماقبل آن	تاکنون برای رفع آسیب‌پذیری فوق راه حلی ارائه نگردیده است.	goo.gl/OcfLaC goo.gl/WrKKbK

نرم‌افزارهای کاربردی

موضوع	شناسه	منبع	تاریخ انتشار	سطح خطر	خلاصه‌ای از آسیب‌پذیری	نحوه رفع	اطلاعات بیشتر
Microsoft Office	MS16-133	goo.gl/mQScms	2016-11-08	متوسط	چندین آسیب‌پذیری اجرای کد از راه دور در Microsoft Office در صورت باز کردن یک فایل Office جعلی در ویندوز و مک	برای Office 2013 64bit : goo.gl/37NySt برای Office 2016 64bit روی مک : goo.gl/UvkjUy	goo.gl/mQScms
NVIDIA	CVE-2016-8812 CVE-2016-8811 CVE-2016-8810 , …	goo.gl/mJPuQS goo.gl/RJH7B8 goo.gl/FMpLwa	2016-11-02	متوسط	چندین آسیب‌پذیری جلوگیری از سرویس و اجرای کد در درایور گرافیک NVIDIA روی ویندوز و لینوکس و همچنین در Quadro، NVIDIA NVS و Geforce روی سیستم‌های مبتنی بر ویندوز	آسیب‌پذیری‌های فوق در نسخه‌های 342.00، 375.63، 304.132 و غیره برطرف گردیده است. goo.gl/LGhxO	goo.gl/YqeFZ9 goo.gl/Vh6Wuq goo.gl/cfgCeQ , …

OpenJPEG	CVE-2016-9118 CVE-2016-9117 CVE-2016-9116 , …	goo.gl/hY1axS goo.gl/J53Ug4 goo.gl/BgMu4Q , …	2016-10-30	متوسط	چندین آسیب‌پذیری سرریزی بافر مبتنی بر هیپ و جلوگیری از سرویس در OpenJPEG نسخه‌ی 2.1.2	تاکنون راه حلی برای رفع آسیب‌پذیری فوق ارائه نگردیده است.	goo.gl/8nOcts goo.gl/yoot5e goo.gl/LDBcDC , …
Adobe Acrobat, Reader	APSB16-33	goo.gl/qpcBeo	2016-10-21	زیاد	چندین آسیب‌پذیری جلوگیری از سرویس در Acrobat DC و Acrobat Reader DC نسخه‌های Continuous و Classic و در Acrobat XI و Reader XI	آسیب‌پذیری فوق در Acrobat DC و Acrobat Reader DC نسخه‌های Continuous و Classic به ترتیب در نسخه‌های 15.020.20039 و 15.006.30243 و در Acrobat XI و Reader XI نسخه‌ی 11.0.18 برطرف گردیده است. goo.gl/9E1Y6	goo.gl/xW84o2 goo.gl/LWdo4V goo.gl/yrqbqj , …
Foxit Reader, PhantomPDF	CVE-2016-8879 CVE-2016-8878 CVE-2016-8877 , …	goo.gl/dv9l1W	2016-10-18	زیاد	چندین آسیب‌پذیری اجرای کد از راه دور و جلوگیری از سرویس در Foxit Reader و PhantomPDF نسخه‌های 8.05 و ماقبل آن در ویندوز و نسخه‌های 2.1.0.0805 و ماقبل آن در لینوکس و نسخه‌های 2.1.0.0804 و ماقبل آن در مک	آسیب‌پذیری‌های فوق در Foxit Reader و PhantomPDF نسخه‌ی 8.1 در ویندوز و نسخه‌ی 2.2 در لینوکس و مک برطرف گردیده است. goo.gl/XQOnb	goo.gl/5eAWIE goo.gl/HNEdAE goo.gl/LjUlEL , …
libav	CVE-2016-7424	goo.gl/6kjvM1	2016-10-11	متوسط	آسیب‌پذیری جلوگیری از سرویس در libav نسخه‌ی 11.7 به واسطه‌ی نقص در عملکرد تابع put_no_rnd_pixels8_xy2_mmx با استفاده از یک فایل MP3 جعلی	برای رفع مشکل فوق در Debian Jessie از libav نسخه‌ی 6:11.8-1~deb8u1 استفاده نمائید. goo.gl/kYI2sv	goo.gl/sQXU0F
Microsoft Office	MS16-121	goo.gl/gaqRGg	2016-10-11	زیاد	آسیب‌پذیری اجرای کد از راه دور در Microsoft Office به واسطه‌ی وجود نقص در مدیریت مناسب فایل‌های RTF در ویندوز و مک	برای Office 2013 32bit : goo.gl/OwVSJF برای Office 2011 روی مک : goo.gl/rZS7Fg	goo.gl/muwmBN

Adobe Flash Player	APSB16-37	goo.gl/1bnwcC	2016-11-08	زیاد	چندین آسیب‌پذیری اجرای کد دلخواه در Adobe Flash Player در سیستم‌های عامل ویندوز، لینوکس و مک	این آسیب‌پذیری‌ها در Adobe Flash Player نسخه‌ی 23.0.0.207 در ویندوز و مک و نسخه‌ی 11.2.202.644 در لینوکس برطرف گردیده است. goo.gl/qDW9E مرورگرهای Internet Explorer، Microsoft Edge و Google Chrome را به‌روزرسانی کنید. ویندوزهای 8.1 و 10 را به‌روزرسانی نمائید.	goo.gl/P3aONw goo.gl/cwkSXz goo.gl/LQBo0Q , …
libcurl	CVE-2016-7167	goo.gl/rbUxEA	2016-09-14	زیاد	چندین آسیب‌پذیری سرریزی بافر مقدار عدد صحیح در libcurl نسخه‌های ماقبل 7.50.3 به واسطه‌ی نقص در عملکرد توابع curl_escape، curl_easy_escape، curl_unescape و curl_easy_unescape	آسیب‌پذیری‌های فوق در libcurl نسخه‌ی 7.50.3 برطرف گردیده است. goo.gl/mtuO9a	goo.gl/YWe81i