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	2.4.34	2018-07-16	goo.gl/ySdR
Squid Proxy & Cache Server	3.5.28	2018-07-15	goo.gl/ZCyZ6f

آسیب‌پذیری‌ها

موضوع	شناسه	منبع	تاریخ انتشار	سطح خطر	خلاصه‌ای از آسیب‌پذیری	نحوه رفع	اطلاعات بیشتر
Microsoft Exchange Server	CVE-2018-8374 CVE-2018-8302	goo.gl/WeLsPh goo.gl/UZgYKn	2018-08-14	زیاد	آسیب‌پذیری‌های Tampering، اجرای کد از راه دور و افزایش سطح دسترسی در Microsoft Exchange Server	برای Exchange Server 2010 CU10 : goo.gl/JkJJwL برای Exchange Server 2013 CU20 : goo.gl/yDXBs4	goo.gl/5YGxxt goo.gl/aueXei
Active Directory Federation Services	CVE-2018-8340	goo.gl/Mbu1LL	2018-08-14	متوسط	آسیب‌پذیری دور زدن محدودیت‌های امنیتی در Active Directory Federation Services به واسطه‌ی مدیریت نادرست درخواست‌های احراز هویت چندعامله با استفاده از ارسال یک درخواست احراز هویت جعلی	برای ویندوزهای 8.1 ,32 ,64bit و Server 2012 R2 : goo.gl/hGBGzm برای ویندوزهای 10 ,1607 ,32 64bit و Server 2016 : goo.gl/7f7KjF	goo.gl/pkgFC1

Microsoft SQL Server	CVE-2018-8273	goo.gl/ZwYqtQ	2018-08-14	زیاد	آسیب‌پذیری سرریزی بافر و اجرای کد در Microsoft SQL Server با ارسال یک query جعلی	برای SQL Server 2016 SP2 64bit : goo.gl/kynhav برای SQL Server 2017 64bit : goo.gl/671H5E	goo.gl/LRtJWX
Samba	CVE-2018-1139	goo.gl/TNzXAj	2018-07-26	----	آسیب‌پذیری آشکارسازی اطلاعات حساس توسط مهاجم MiTM در Samba به واسطه‌ی ضعف موجود در احراز هویت NTLMv1 حتی در صورت غیرفعال بودن آن	آسیب‌پذیری فوق در Samba نسخه‌های 4.7.9 و 4.8.4 برطرف گردیده است. goo.gl/EqEgxM	goo.gl/XxcKBq
Apache HTTP Server	CVE-2018-1312 CVE-2018-1303 CVE-2018-1302 , ...	goo.gl/hjt3yG goo.gl/QvARhv goo.gl/ci1PrQ , ...	2018-03-26	---	چندین آسیب‌پذیری جلوگیری از سرویس و دور زدن محدودیت‌های امنیتی در سرویس‌دهنده‌ی Apache HTTP Server نسخه‌های ماقبل 2.4.30	آسیب‌پذیری‌های فوق در Apache HTTP Server نسخه‌ی 2.4.30 برطرف گردیده است. goo.gl/ySdR	goo.gl/EQ6wav goo.gl/Z6MMTY goo.gl/MDcCPJ , ...

سیستم‌های عامل

موضوع	شناسه	منبع	تاریخ انتشار	سطح خطر	خلاصه‌ای از آسیب‌پذیری	نحوه رفع	اطلاعات بیشتر
Linux	CVE-2018-16658	goo.gl/f8m3jd	2018-09-05	----	آسیب‌پذیری نشت اطلاعات در هسته‌ی لینوکس به واسطه‌ی وجود نقص در عملکرد فایل drivers/cdrom/cdrom.c و خواندن حافظه‌ی هسته‌ی لینوکس	آسیب‌پذیری فوق در هسته‌ی لینوکس نسخه‌ی 4.18.6 برطرف گردیده است. goo.gl/q78o37	goo.gl/72jhj7
Windows	CVE-2018-8414	goo.gl/fQeVjW	2018-08-14	متوسط	آسیب‌پذیری اجرای کد دلخواه در ویندوز به واسطه‌ی عدم اعتبارسنجی مناسب مسیرهای فایل توسط Windows Shell با استفاده از ترغیب کاربر به باز کردن یک فایل جعلی	برای ویندوزهای 10 1803 32, 64bit و Server 2016 1803 64bit : goo.gl/LN3HuX	goo.gl/qmuex5

Windows	CVE-2018-8406 CVE-2018-8405 CVE-2018-8401 CVE-2018-8400	goo.gl/CyuhrD goo.gl/M5ehxL goo.gl/sfzA8X goo.gl/L262qn	2018-08-14	متوسط	چندین آسیب‌پذیری افزایش سطح دسترسی در ویندوز به واسطه‌ی مدیریت نامناسب اشیاء در حافظه توسط درایور DXGKRNL	برای ویندوزهای 1607 10 و Server 2016 : goo.gl/rP1B6u برای ویندوزهای 32, 1803 10 64bit و Server 2016 1803 64bit : goo.gl/LN3HuX	goo.gl/2CmNmG goo.gl/4iFHyT goo.gl/rQytuL goo.gl/ZAZZxB
Windows	CVE-2018-8404 CVE-2018-8399	goo.gl/cSrp3Y goo.gl/MjnNxq	2018-08-14	متوسط	آسیب‌پذیری‌های افزایش سطح دسترسی و اجرای کد دلخواه در ویندوز به واسطه‌ی عدم مدیریت صحیح اشیاء در حافظه توسط کامپوننت Win32k	برای ویندوز 32, 64bit 1703 : goo.gl/mwsFdX برای ویندوزهای 32, 64bit 7 و Server 2008 R2 : goo.gl/jg84kU	goo.gl/eV58te goo.gl/JVpaZ3
Windows	CVE-2018-8398 CVE-2018-8397 CVE-2018-8396 CVE-2018-8394	goo.gl/rA28jv goo.gl/Ztztnu goo.gl/Y9vJ7d goo.gl/1Cuz4A	2018-08-14	متوسط	چندین آسیب‌پذیری آشکارسازی اطلاعات و اجرای کد از راه دور در ویندوز به واسطه‌ی عدم مدیریت صحیح اشیاء در حافظه توسط Windows GDI	برای ویندوزهای 32, 64bit 8.1 و Server 2012 R2 : goo.gl/wSkBZm برای ویندوزهای 32, 64bit 7 و Server 2008 R2 : goo.gl/jg84kU	goo.gl/nPp1Vt goo.gl/EFXLdW goo.gl/QSr6Tu goo.gl/TvyEMn
Windows	CVE-2018-8349	goo.gl/QJPRbD	2018-08-14	متوسط	آسیب‌پذیری اجرای کد از راه دور در ویندوز به واسطه‌ی عدم پاک‌سازی مناسب اشیاء در حافظه توسط Microsoft COM با ترغیب قربانی به باز کردن یک فایل جعلی	برای ویندوزهای 32, 1803 10 64bit و Server 2016 1803 : goo.gl/wViUZ8 برای ویندوزهای 32, 64bit 8.1 و Server 2012 R2 : goo.gl/LTf7kJ	goo.gl/RYPoSP
Windows	CVE-2018-8348 CVE-2018-8347 CVE-2018-8341	goo.gl/Uf1iDW goo.gl/7VE5tf goo.gl/7Z9Bq9	2018-08-14	متوسط	آسیب‌پذیری‌های آشکارسازی اطلاعات، اجرای کد و افزایش سطح دسترسی در ویندوز به واسطه‌ی عدم تجزیه مناسب لینک‌های symbolic خاص و همچنین مدیریت نامناسب اشیاء در حافظه توسط هسته‌ی ویندوز	برای ویندوزهای 32, 64bit 7 SP1 و Server 2008 R2 : goo.gl/rRET4P برای ویندوزهای 32, 1607 10 64bit و Server 2016 : goo.gl/Ca8TdW	goo.gl/GDNy4M goo.gl/p2VWZ2 goo.gl/hVduzH

Windows	CVE-2018-8339	goo.gl/kyYxwZ	2018-08-14	متوسط	آسیب‌پذیری افـزایش سـطح دسترسـی و اجـرای کـد دلخواه در ویندوز به واسـطه‌ی پـاک‌سـازی نامناسـب ورودی توسط Windows Installer	بـرای ویـنـدوزهای 8.1 ,32 ,64bit و Server 2012 R2 : goo.gl/LTf7kJ برای ویندوزهای 7 SP1 ,32 ,64bit و Server 2008 R2 : goo.gl/rRET4P	goo.gl/kN4riz
Windows	CVE-2018-8253	goo.gl/g2Ssz1	2018-08-14	متوسط	آسیب‌پذیری افـزایش سـطح دسترسـی در ویـنـدوز در صورت فعال بـودن Microsoft Cortana و مـرور وب‌سایت در lockscreen	بـرای ویـنـدوزهای 10 ,1607 ,32, 64bit و Server 2016 : goo.gl/Ca8TdW	goo.gl/si5h1q
Windows	CVE-2018-8204 CVE-2018-8200	oo.gl/ao6Xvh goo.gl/vxW8Z2	2018-08-14	متوسط	آسـیب‌پـذیری دور زدن محـدودیت‌هـای امنیتـی در ویندوز در صورت دسترسی به سیستم قربانی و تزریق کد مخرب در یـک اسـکریپت مـورد اعتمـاد سیاسـت امنیتی Code Integrity	بـرای ویـنـدوزهای 10 ,1703 ,32, 64bit : goo.gl/MTZqsZ بـرای ویـنـدوزهای 10 ,1709 ,32, 64bit و Server 2016 1709 : goo.gl/PRBcYd	goo.gl/gHEpCr goo.gl/J6eWSE

محیط‌های برنامه‌نویسی

دریافت آخرین نسخه‌ی پایدار

موضوع	آخرین نسخه پایدار	تاریخ عرضه	لینک دریافت
Joomla!	**3.8.12**	**2018-08-28**	**goo.gl/bWF9px**
Drupal	**8.6.0**	**2018-09-05**	**goo.gl/c5F8At**
WordPress	**4.9.8**	**2018-08-02**	**goo.gl/DK0Wx**

آسیب‌پذیری‌ها

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

Joomla!	CVE-2018-15882 CVE-2018-15881 CVE-2018-15880	goo.gl/6RsUwF goo.gl/c4MjNB goo.gl/HAE6NJ	2018-08-28	کم	آسیب‌پذیری‌های دور زدن محدودیت‌های امنیتی و XSS در Joomla! نسخه‌های ماقبل 3.8.12	آسیب‌پذیری‌های فوق در Joomla! نسخه‌ی 3.8.12 برطرف گردیده است. goo.gl/bWF9px	goo.gl/ALwaih goo.gl/Ef75ig goo.gl/QGzWQg
Microsoft .NET Framework	CVE-2018-8360	goo.gl/hkLpbg	2018-08-14	متوسط	آسیب‌پذیری آشکارسازی اطلاعات در Microsoft .NET Framework. نسخه‌های مختلف در صورت استفاده از آن در شبکه‌های با حجم ارتباطات بسیار بالا	برای .NET Framework. نسخه‌ی 4.7.2 روی ویندوزهای 10 1803 32, 64bit و Server 2016 : 1803 goo.gl/hRMNKK	goo.gl/uUibvL
PHP	CVE-2018-15132 CVE-2018-14883	goo.gl/Y1HQdg goo.gl/1oh1t5	2018-08-07	----	آسیب‌پذیری‌های افزایش سطح دسترسی وخواندن بافر مبتنی بر هیپ در PHP به واسطه‌ی وجود نقص در عملکرد link_win32.c و exif.c	آسیب‌پذیری‌های فوق در PHP نسخه‌های 7.2.8، 7.1.20، 7.0.31 و 5.6.37 برطرف گردیده است. goo.gl/GjgUex	goo.gl/786Fso goo.gl/WSbzV1
DotNetNuke	CVE-2017-0929	goo.gl/AiQirf	2018-07-03	----	آسیب‌پذیری SSRF و دسترسی به اطلاعات منابع شبکه در DNN به واسطه‌ی وجود نقص در عملکرد کلاس DnnImageHandler	آسیب‌پذیری فوق در DNN نسخه‌ی 9.2.0 برطرف گردیده است. goo.gl/xXn6oB	goo.gl/8cikeb
Drupal	CVE-2017-6922 CVE-2017-6921 CVE-2017-6920	goo.gl/kF9uGR	2017-06-21	متوسط	آسیب‌پذیری‌های اجرای کد از راه دور و افزایش سطح دسترسی در Drupal نسخه‌های مختلف	آسیب‌پذیری‌های فوق در Drupal نسخه‌های 8.3.4 و 7.56 برطرف گردیده است. goo.gl/c5F8At	goo.gl/MkPF96
Yii Framework	CVE-2018-8074 CVE-2018-8073 CVE-2018-7269	goo.gl/ZPd2GV	2018-03-20	----	آسیب‌پذیری‌های اجرای کد و تزریق SQL در Yii Framework نسخه‌های 2.x الی ماقبل 2.0.15	آسیب‌پذیری‌های فوق در Yii Framework نسخه‌های 2.0.15 برطرف گردیده است.	goo.gl/HDEkfY goo.gl/HoXba7 goo.gl/8FAVHb

مرورگرهای اینترنت

دریافت آخرین نسخه‌ی پایدار

موضوع	آخرین نسخه پایدار	تاریخ عرضه	لینک دریافت
Mozilla Firefox	**62.0.5**	**2018-09-05**	**goo.gl/yIXtW**
Google Chrome	**69.0.3497.81**	**2018-09-04**	**goo.gl/Jk2diZ**

آسیب‌پذیری‌ها

موضوع	شناسه	منبع	تاریخ انتشار	سطح خطر	خلاصه‌ای از آسیب‌پذیری	نحوه رفع	اطلاعات بیشتر
Microsoft Edge	CVE-2018-8390 CVE-2018-8388 , …	goo.gl/UdU5Y4 goo.gl/KPp1B1 , …	2018-08-14	متوسط	چندین آسیب‌پذیری جعل، اجرای کد از راه دور و افزایش سطح دسترسی در مرورگر Microsoft Edge	برای مرورگر Microsoft Edge روی ویندوزهای 10 1803 32, 64bit و Server 2016 1803 : goo.gl/wtGyhc	goo.gl/4Ux6GM goo.gl/K7rcKB , …
Internet Explorer	CVE-2018-8389 CVE-2018-8385 , …	goo.gl/ME6P1C goo.gl/F3y2kL , …	2018-08-14	زیاد	چندین آسیب‌پذیری اجرای کد از راه دور، افزایش سطح دسترسی در مرورگر Internet Explorer با ترغیب قربانی به مشاهده‌ی یک وب‌سایت جعلی	برای مرورگر Internet Explorer 11 روی ویندوزهای 8.1 32, 64bit و Server 2012 R2 : goo.gl/4rDS4d	goo.gl/XRXMNX goo.gl/SjaSxu , …
Google Chrome	CVE-2017-15429	goo.gl/NnJmMP	2017-12-14	---	آسیب‌پذیری UXSS در مرورگر Google Chrome با استفاده از یک صفحه‌ی HTML جعلی	آسیب‌پذیری فوق در مرورگر Google Chrome نسخه‌ی 63.0.3239.108 برطرف گردیده است. goo.gl/Jk2diZ	goo.gl/5gFToc

مجازی‌سازی

دریافت آخرین نسخه‌ی پایدار

موضوع	آخرین نسخه پایدار	تاریخ عرضه	لینک دریافت
VirtualBox	5.2.18	2018-08-14	goo.gl/l3wrf

آسیب‌پذیری‌ها

موضوع	شناسه	منبع	تاریخ انتشار	سطح خطر	خلاصه‌ای از آسیب‌پذیری	نحوه رفع	اطلاعات بیشتر
VMware Horizon	CVE-2018-6970	goo.gl/mM9YQn	2018-08-14	متوسط	آسیب‌پذیری نشت اطلاعات در VMware Horizon به واسطه‌ی امکان خواندن خارج از محدوده‌ی مشخص شده در حافظه	برای رفع مشکل می‌بایست حداقل از Horizon 6 نسخه‌ی 6.2.7، Horizon 7 نسخه‌ی 7.5.1 و Horizon Client نسخه‌ی 4.8.1 استفاده نمود.	goo.gl/a2BMJj
VMware ESXi, Workstation, Fusion	CVE-2018-6972	goo.gl/mV2Qca	2018-07-19	متوسط	آسیب‌پذیری جلوگیری از سرویس در VMware ESXi، Workstation و Fusion	آسیب‌پذیری فوق در ESXi نسخه‌های ESXi670-201806401-BG، ESXi650-201806401-BG، ESXi600-201806401-BG و ESXi550-201806401-BG، Workstation نسخه‌ی 14.1.2 و Fusion نسخه‌ی 10.1.2 برطرف گردیده است.	goo.gl/Bg6nSy

تجهیزات شبکه، دیواره‌های آتش و ضدبدافزار

موضوع	شناسه	منبع	تاریخ انتشار	سطح خطر	خلاصه‌ای از آسیب‌پذیری	نحوه رفع	اطلاعات بیشتر
Trend Micro Security 2018	CVE-2018-15363 CVE-2018-10514 CVE-2018-10513	goo.gl/Cq9RUD	2018-08-30	زیاد	چندین آسیب‌پذیری افزایش سطح دسترسی در محصولات مختلف Trend Micro Security 2018 (Premium Security، Maximum Security، Internet Security و Antivirus) نسخه‌های 12.0 و ماقبل آن	آسیب‌پذیری‌های فوق در نسخه‌ی 12.0.1226 برطرف گردیده است.	goo.gl/oe6kcU goo.gl/mezF6S goo.gl/R7ZHEL

Mikrotik RouterOS	CVE-2018-1159 CVE-2018-1158 CVE-2018-1157	goo.gl/HYXrDT	2018-08-22	زیاد	چندین آسیب‌پذیری خرابی حافظه وجلوگیری از سرویس در Mikrotik RouterOS	آسیب‌پذیری‌های فوق در نسخه‌های 6.43، 6.42.7 و 6.40.9 برطرف گردیده است. goo.gl/fVtDHr	goo.gl/FD8qtu goo.gl/NRJw7J goo.gl/p2U32M
Cisco Web Security Appliance	CVE-2018-0428	goo.gl/aZNudY	2018-08-15	متوسط	آسیب‌پذیری افزایش سطح دسترسی در Cisco WSA به واسطه‌ی وجود نقص در عملکرد زیرسیستم مدیریت اکانت و پیاده‌سازی نادرست کنترل دسترسی	آسیب‌پذیری فوق در Cisco WSA با نسخه‌های نرم‌افزاری 11.5.1-115، 10.5.2-072 و 10.1.3-054 برطرف گردیده است. goo.gl/1p3VFD	goo.gl/rBt4Lg
Cisco IOS, IOS XE	CVE-2018-0131	goo.gl/nc5JaG	2018-08-13	متوسط	آسیب‌پذیری افزایش سطح دسترسی در Cisco IOS و IOS XE نسخه‌ی 15.5(3)S و به دست آوردن nonce رمزنگاری شده‌ی مورد استفاده در RSA به واسطه‌ی پیاده‌سازی نادرست IKEv1	آسیب‌پذیری فوق در Cisco IOS و IOS XE نسخه‌های 15.5(3)S8، 16.3.6، 16.6.3 و غیره برطرف گردیده است. goo.gl/Mw97u9	goo.gl/jN1iZo
HPE iLO	CVE-2018-7093 CVE-2018-7078 CVE-2017-8987 CVE-2016-4406	goo.gl/RPr5uU goo.gl/FfKjkk goo.gl/7T6mBw goo.gl/9wWk2H	2018-08-07	زیاد	چندین آسیب‌پذیری اجرای کد از راه دور، جلوگیری از سرویس و XSS در HPE iLO نسخه‌های مختلف	آسیب‌پذیری‌های فوق در HPE iLO 4 نسخه‌ی 2.60 و در HPE iLO 5 نسخه‌ی 1.30 برطرف گردیده است.	goo.gl/AP6Kc1 goo.gl/AFcVyS goo.gl/JiPkMz goo.gl/twnxSc
McAfee Data Loss Prevention	CVE-2018-6683	goo.gl/zQvkVe	2018-07-24	زیاد	آسیب‌پذیری دور زدن محدودیت‌های امنیتی در McAfee DLP با تغییر فایل‌های پالیسی محلی به واسطه‌ی پیکربندی نادرست سطوح کنترل دسترسی	آسیب‌پذیری فوق در McAfee DLP نسخه‌های 10.0.500 و 11.0.400 برطرف گردیده است.	goo.gl/dACPDp
ClamAV	CVE-2018-0361 CVE-2018-0360 CVE-2017-16932	goo.gl/Daj8QN	2018-07-09	----	آسیب‌پذیری جلوگیری از سرویس (لوپ بی‌نهایت و صرف زمان زیاد در تجزیه فایل‌های کوچک) در ClamAV به واسطه‌ی وجود سرریزی مقدار عدد صحیح و همچنین عدم بررسی طول فایل‌های PDF	آسیب‌پذیری فوق در ClamAV نسخه‌ی 0.100.1 برطرف گردیده است. goo.gl/eNJDFn	goo.gl/tp31Pt goo.gl/DmgmSb goo.gl/iTCbVs

Fortinet	CVE-2017-17541	goo.gl/2cqMNc	2018-07-05	----	آسیب‌پذیری تزریق کد جاوااسکریپت و HTML در FortiManager Fortinet و FortiAnalyzer نسخه‌های 6.0.0 و 5.6.4 بواسطه‌ی وجود XSS	آسیب‌پذیری فوق در نسخه‌های 6.0.1 و 5.6.5 برطرف گردیده است.	goo.gl/HAqyCL
Symantec Endpoint Protection	CVE-2018-5237 CVE-2018-5236	goo.gl/9KbMSW	2018-06-12	متوسط	آسیب‌پذیری‌های Race Condition و افزایش سطح دسترسی در Symantec Endpoint Protection	آسیب‌پذیری‌های فوق در نسخه‌های 14 RU1 MP1 و 12.1 RU6 MP10 برطرف گردیده است.	goo.gl/cbkCBG goo.gl/czaLYE

نرم‌افزارهای کاربردی

موضوع	شناسه	منبع	تاریخ انتشار	سطح خطر	خلاصه‌ای از آسیب‌پذیری	نحوه رفع	اطلاعات بیشتر
Dameware Mini Remote Control	CVE-2018-12897	goo.gl/kgsTZA	2018-09-05	----	آسیب‌پذیری سرریزی بافر در Dameware Mini Remote Control نسخه‌ی 12.0.5 به واسطه‌ی مدیریت ناامن ورودی کاربر	آسیب‌پذیری فوق در نسخه‌ی 12.1 برطرف گردیده است. goo.gl/HH6fhw	goo.gl/hC898d
OpenSSH	CVE-2018-15919	goo.gl/FjWSAH	2018-08-27	----	آسیب‌پذیری آشکارسازی اطلاعات در OpenSSH به واسطه‌ی رفتار قابل مشاهده‌ی فایل auth-gss2.c از راه دور	هنوز راه حلی برای رفع آسیب‌پذیری فوق ارائه نگردیده است.	goo.gl/erNL6u
Adobe Photoshop CC	APSB18-28	goo.gl/PeshDy	2018-08-21	زیاد	آسیب‌پذیری خرابی حافظه و اجرای کد از راه دور در Adobe Photoshop CC نسخه‌های 2018 19.1.5 و ماقبل آن و 2017 18.1.5 و ماقبل آن	آسیب‌پذیری‌های فوق در نسخه‌های 2017 18.1.6 و 2018 19.1.6 برطرف گردیده است.	goo.gl/y6G3rv goo.gl/xGPgnq
phpMyAdmin	CVE-2018-15605	goo.gl/4Uj6DA	2018-08-21	متوسط	یک آسیب‌پذیری XSS در phpMyAdmin با استفاده از یک فایل جعلی جهت دستکاری اطلاعات حین بارگزاری فایل توسط کاربر احراز هویت شده	آسیب‌پذیری فوق در phpMyAdmin نسخه‌ی 4.8.3 برطرف گردیده است. goo.gl/qUrxc9	goo.gl/hhySjg

Adobe Acrobat, Reader	APSB18-29	goo.gl/YpQUaf	2018-08-21	زیاد	آسیب‌پذیری اجرای کد دلخواه از راه دور در Acrobat DC و Acrobat Reader DC نسخه‌های Continuous و Classic در ویندوز و مک	آسیب‌پذیری فوق در Acrobat DC و Acrobat Reader DC نسخه‌ی Continuous در نسخه‌ی 2018.011.20058 و در Acrobat 2017 و Acrobat Reader 2017 نسخه‌ی Classic در نسخه‌ی 2017.011.30099 برطرف گردیده است. goo.gl/9E1Y6	goo.gl/2HyzHE goo.gl/cCF4DY
Adobe Flash Player	APSB18-25	goo.gl/3ykxkM	2018-08-14	متوسط	چندین آسیب‌پذیری افزایش سطح دسترسی، آشکارسازی اطلاعات و دور زدن محدودیت‌های امنیتی در Adobe Flash Player در سیستم‌های عامل ویندوز، لینوکس، مک و Chrome OS	این آسیب‌پذیری‌ها در Adobe Flash Player نسخه‌ی 30.0.0.154 در ویندوز، مک، لینوکس و Chrome OS 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/znNkC7 goo.gl/2cb1pA , …
PostgreSQL	CVE-2018-10925 CVE-2018-10915	goo.gl/DqbA6s	2018-08-14	----	آسیب‌پذیری‌های دسترسی به اطلاعات حساس و افزایش سطح دسترسی در PostgreSQL به واسطه‌ی نقص موجود در libpq و همچنین سوءاستفاده در صورت داشتن دسترسی ایجاد جدول	آسیب‌پذیری‌های فوق در PostgreSQL نسخه‌های 10.5، 9.6.10، 9.5.14، 9.4.19 و 9.3.24 برطرف گردیده است. goo.gl/QST5us	goo.gl/N3xMCA goo.gl/V4aGx1
Microsoft AutoUpdate	CVE-2018-8412	goo.gl/54zamm	2018-08-14	متوسط	آسیب‌پذیری اجرای کد و افزایش سطح دسترسی در Microsoft AutoUpdate به واسطه‌ی اعتبارسنجی نامناسب قایل‌های به‌روزرسانی قبل از اجرای آن‌ها در مک	برای Microsoft Office 2016 روی مک : goo.gl/776BwV	goo.gl/Znj8qZ

Microsoft Excel	CVE-2018-8382 CVE-2018-8379 CVE-2018-8375	goo.gl/bzsxwb goo.gl/xQeaBf goo.gl/nggACV	2018-08-14	متوسط	آسیب‌پذیری‌های اجرای کد از راه دور، آشکارسازی اطلاعات در Microsoft Excel با استفاده از ترغیب قربانی به باز کردن یک فایل جعلی	برای Microsoft Excel 2016 64bit : goo.gl/rvRhVM برای Microsoft Excel 2013 32bit : goo.gl/wo3byU	goo.gl/xocbgK goo.gl/SPtDj6 goo.gl/M7ZVdH
Microsoft Office	CVE-2018-8378	goo.gl/3DMrG4	2018-08-14	متوسط	آسیب‌پذیری آشکارسازی اطلاعات در Microsoft Office در صورت باز کردن یک فایل جعلی توسط یکی از نرم‌افزارهای Microsoft Office آسیب‌پذیر	برای Microsoft Office 2016 32bit : goo.gl/JP6AQm برای Microsoft Office 2016 64bit : goo.gl/ZyNFTN	goo.gl/FMdWdE
Microsoft PowerPoint	CVE-2018-8376	goo.gl/wkbqWe	2018-08-14	متوسط	آسیب‌پذیری اجرای کد از راه دور در Microsoft PowerPoint به واسطه‌ی مدیریت نامناسب اشیاء در حافظه در صورت باز کردن یک فایل جعلی	برای Microsoft PowerPoint 2010 32bit : goo.gl/88Hc3w برای Microsoft PowerPoint 2010 64bit : goo.gl/adp5Tp	goo.gl/AR7znt
Nmap	CVE-2018-15173	goo.gl/mD5t3y	2018-08-07	----	آسیب‌پذیری جلوگیری از سرویس در Nmap نسخه‌ی 7.70 و ماقبل آن در صورت استفاده از سوئیچ sV- با استفاده از یک سرویس مبتنی بر TCP جعلی	تاکنون راه حلی برای رفع این آسیب‌پذیری ارائه نگردیده است.	goo.gl/VM381v
HPE iLO	CVE-2018-7093 CVE-2018-7078	goo.gl/54gK4B goo.gl/YQDG5t	2018-08-07	متوسط	آسیب‌پذیری جلوگیری از سرویس و اجرای کد از راه دور در HPE iLO 5 نسخه‌های ماقبل 1.30، iLO 4 نسخه‌های ماقبل 2.60 و iLO 3 نسخه‌های ماقبل 1.90	آسیب‌پذیری‌های فوق در HPE iLO 5 نسخه‌ی 1.30، iLO 4 نسخه‌ی 2.60 و iLO 3 نسخه‌ی 1.90 برطرف گردیده است.	goo.gl/4sddRb goo.gl/vkj8GF
SquirrelMail	CVE-2018-14955 CVE-2018-14954 , …	goo.gl/cmSyq7 goo.gl/tZaT8d , …	2018-08-05	----	چندین آسیب‌پذیری اجرای اسکریپت و کد دلخواه در SquirrelMail تا نسخه‌ی 1.4.22 به واسطه‌ی وجود XSS در صفحه‌ی نمایش متن ایمیل	تاکنون راه حلی برای رفع این آسیب‌پذیری ارائه نگردیده است.	goo.gl/L1pUdT goo.gl/z79qCT , …

PRTG Network Monitor	CVE-2018-9276	goo.gl/sJh3u3	2018-06-27	----	آسیب‌پذیری تزریق دستور در PRTG Network Monitor نسخه‌های ماقبل 18.2.39 در صورت داشتن دسترسی مدیریتی به کنسول وب	آسیب‌پذیری فوق در PRTG Network Monitor نسخه‌ی 18.2.39 برطرف گردیده است. goo.gl/ReUzgZ	goo.gl/Dx5Rbb
PRTG Network Monitor	CVE-2018-10253	goo.gl/zvYp8e	2018-04-20	زیاد	آسیب‌پذیری جلوگیری از سرویس در PRTG Network Monitor به واسطه‌ی مدیریت نادرست حافظه‌ی Stack هنگام فراخوانی API نامشخص	آسیب‌پذیری فوق در نسخه‌ی 18.1.39.1648 برطرف گردیده است. goo.gl/mPQvxv	goo.gl/4MGRGR
FreeNAS	CVE-2014-5334	goo.gl/Y1S2uF	2018-01-08	----	آسیب‌پذیری افزایش سطح دسترسی در FreeNAS به واسطه‌ی عدم وجود کلمه عبور روی کاربر Admin به صورت پیش‌فرض	آسیب‌پذیری فوق در FreeNAS نسخه ی 9.3-M3 برطرف گردیده است. goo.gl/pXnhqb	goo.gl/FMqSZD