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	2.4.37	2018-10-23	goo.gl/ySdR
Squid Proxy & Cache Server	4.4	2018-10-27	goo.gl/JRPoY4

آسیب‌پذیری‌ها

موضوع	شناسه	منبع	تاریخ انتشار	سطح خطر	خلاصه‌ای از آسیب‌پذیری	نحوه رفع	اطلاعات بیشتر
Microsoft Exchange Server	CVE-2018-8581	goo.gl/NyeKkM	2018-11-13	متوسط	آسیب‌پذیری جعل هویت و افزایش سطح دسترسی در Microsoft Exchange Server با استفاده از یک حمله‌ی MiTM برای ارجاع یک درخواست احراز هویت به سمت سرور	تاکنون راه حلی برای رفع این آسیب‌پذیری ارائه نشده است.	goo.gl/Qmrk5R
Microsoft SharePoint Server	CVE-2018-8578 CVE-2018-8572 , …	goo.gl/rYh5vw goo.gl/Hm3ALb , …	2018-11-13	متوسط	چندین آسیب‌پذیری آشکارسازی اطلاعات، افزایش سطح دسترسی و اجرای کد از راه دور در Microsoft SharePoint Server به واسطه‌ی عدم پاک‌سازی مناسب درخواست وب جعلی، عدم مدیریت صحیح اشیاء در حافظه و غیره	برای Microsoft SharePoint Enterprise Server 2016 : goo.gl/6K7W4P برای Microsoft SharePoint Server 2019 : goo.gl/YrMwVv	goo.gl/KDhFuU goo.gl/fkPtwy , …

Active Directory Federation Services	CVE-2018-8547	goo.gl/h7DLQ2	2018-11-13	متوسط	آسیب‌پذیری XSS در ویندوز به واسطه‌ی عدم پاک‌سازی مناسب یک درخواست وب جعلی توسط یک نسخه‌ی سفارشی متن‌باز از Microsoft AD FS	برای ویندوزهای Server 2019 و 10 1809 32, 64bit : goo.gl/9XuY6D برای ویندوزهای Server 2012 R2 و 8.1 32, 64bit : goo.gl/jirNmF	goo.gl/q8PLMi
Microsoft Skype for Business	CVE-2018-8546	goo.gl/T6AWBE	2018-11-13	کم	آسیب‌پذیری جلوگیری از سرویس در Microsoft Skype for Business با ارسال تعدادی emoji به سمت سرور آسیب‌پذیر توسط یک کاربر	برای Skype for Business 2016 64bit : goo.gl/2UJSis برای Microsoft Lync 2013 SP1 64bit : goo.gl/f7XcZ7	goo.gl/oo1Bv7
nginx	CVE-2018-16845 CVE-2018-16844 CVE-2018-16843	goo.gl/kLTKZx goo.gl/MQrsqx	2018-11-06	----	آسیب‌پذیری‌های جلوگیری از سرویس و آشکارسازی اطلاعات حساس در nginx به واسطه‌ی وجود نقص در پیاده‌سازی HTTP/2 و نقص در عملکرد ماژول ngx_http_mp4_module	آسیب‌پذیری‌های فوق در نسخه‌های 1.15.6 و 1.14.1 برطرف شده است. goo.gl/uf3uwb	goo.gl/U3Fx25 goo.gl/ym4ghP goo.gl/bGu1qk
Samba	CVE-2016-2123	goo.gl/xo9Qxr	2018-11-01	----	آسیب‌پذیری‌های افزایش سطح دسترسی و جلوگیری از سرویس در Samba به واسطه‌ی وجود نقص در عملکرد روتین ndr_pull_dnsp_name و خرابی حافظه	آسیب‌پذیری‌های فوق در Samba نسخه‌های 4.5.3، 4.4.8 و 4.3.13 برطرف شده است.	goo.gl/GHgRQd
Squid Proxy Cache	CVE-2018-19132 CVE-2018-19131	goo.gl/3f9HMc goo.gl/YDSfBV	2018-10-28	----	آسیب‌پذیری‌های جلوگیری از سرویس و XSS در Squid Proxy Cache به واسطه‌ی خرابی حافظه و نقص در تولید صفحه‌ی خطای HTTP(S) با استفاده از یک بسته‌ی SNMP و یا یک گواهی‌نامه‌ی جعلی X.509	آسیب‌پذیری‌های فوق در Squid Proxy Cache نسخه‌ی 4.4 برطرف شده است. goo.gl/JRPoY4	goo.gl/geX3CJ goo.gl/iG68kX
Hyper-V	CVE-2018-8490 CVE-2018-8489	goo.gl/E6JC2t goo.gl/VnfeUx	2018-10-09	زیاد	آسیب‌پذیری اجرای کد از راه دور در Hyper-V به واسطه‌ی اعتبارسنجی نامناسب ورودی کاربر احراز هویت شده با استفاده از اجرای یک برنامه‌ی کاربردی جعلی	برای ویندوزهای Server 2016 و 10 1607 32, 64bit : goo.gl/JUA6PA برای ویندوزهای Server 2012 R2 و 8.1 32, 64bit : goo.gl/KgZ3JM	goo.gl/ynEE6T goo.gl/XioUL4

Apache HTTP Server	CVE-2018-11763	goo.gl/q5o7Nw	2018-09-25	----	آسیب‌پذیری جلوگیری از سرویس در Apache HTTP Server نسخه‌های 2.4.34 و ماقبل آن با ارسال فریم‌های SETTINGS با حداکثر حجم ممکن به صورت مکرر	آسیب‌پذیری فوق در Apache HTTP Server نسخه‌ی 2.4.35 برطرف شده است. goo.gl/ySdR	goo.gl/GxNMp8

سیستم‌های عامل

موضوع	شناسه	منبع	تاریخ انتشار	سطح خطر	خلاصه‌ای از آسیب‌پذیری	نحوه رفع	اطلاعات بیشتر
Windows	CVE-2018-8592	goo.gl/45ZQXc	2018-11-13	متوسط	آسیب‌پذیری افزایش سطح دسترسی در ویندوز در صورت نصب توسط یک مدیای فیزیکی (CD، USB و غیره) و فعال بودن گزینه‌ی keep nothing در طول فرآیند نصب	برای ویندوزهای Server 2019 و 10 1809 32, 64bit : goo.gl/9XuY6D	goo.gl/ttvDTb
Windows	CVE-2018-8589	goo.gl/DLZNeQ	2018-11-13	متوسط	آسیب‌پذیری افزایش سطح دسترسی و اجرای کد دلخواه در ویندوز به واسطه‌ی مدیریت ناصحیح فراخوانی Win32k.sys با استفاده از اجرای یک برنامه‌ی کاربردی جعلی روی سیستم قربانی	برای ویندوزهای 7 SP1 32, 64bit، Server 2008 R2 : goo.gl/hmmpcK	goo.gl/JqNfJL
Windows	CVE-2018-8584	goo.gl/3yrebh	2018-11-13	متوسط	آسیب‌پذیری افزایش سطح دسترسی و اجرای کد دلخواه در ویندوز به واسطه‌ی فراخوانی نامناسب ALPC با استفاده از اجرای یک برنامه‌ی کاربردی جعلی روی سیستم قربانی	برای ویندوزهای Server 2016 و 10 1803 32, 64bit : goo.gl/FnA1pU برای ویندوزهای Server 2016 و 10 1607 32, 64bit : goo.gl/JX8qMf	goo.gl/EUXD3U
Windows	CVE-2018-8566	goo.gl/HeXwJr	2018-11-13	متوسط	آسیب‌پذیری دورزدن محدودیت‌های امنیتی و دسترسی به اطلاعات حساس در ویندوز به واسطه‌ی عدم توقف مناسب هنگام رمزنگاری توسط BitLocker با خاموش کردن سیستم به صورت فیزیکی هنگام عملیات رمزنگاری	برای ویندوزهای Server 2016 و 10 1803 32, 64bit : goo.gl/ACpgAm برای ویندوزهای Server 2016 و 10 1607 32, 64bit : goo.gl/U5PV2p	goo.gl/22NKxL

Windows	CVE-2018-8563 CVE-2018-8561 CVE-2018-8554 CVE-2018-8485	goo.gl/miF62n goo.gl/vKSbxU goo.gl/t7UjTh goo.gl/uS1Hfe	2018-11-13	متوسط	چندین آسیب‌پذیری آشکارسازی اطلاعات حساس، افزایش سطح دسترسی و اجرای کد دلخواه در ویندوز به واسطه‌ی عدم مدیریت صحیح اشیاء در حافظه توسط DirectX	برای ویندوزهای Server 2012 R2 و 8.1 32, 64bit : goo.gl/jirNmF برای ویندوزهای Server 2019 و 10 1809 32, 64bit : goo.gl/9XuY6D	goo.gl/9U2bLL goo.gl/RVq1VT goo.gl/yF1B1M goo.gl/spo1Td
Windows	CVE-2018-8553	goo.gl/Ap7qqp	2018-11-13	زیاد	آسیب‌پذیری اجرای کد از راه دور در ویندوز به واسطه‌ی عدم مدیریت صحیح اشیاء در حافظه توسط کامپوننت Microsoft Graphics با ترغیب قربانی به باز کردن یک فایل جعلی	برای ویندوزهای 7 SP1 32, 64bit، Server 2008 R2 : goo.gl/hmmpcK برای ویندوزهای Server 2012 R2 و 8.1 32, 64bit : goo.gl/jirNmF	goo.gl/9YGK6c
Windows	CVE-2018-8544	goo.gl/uRTpgM	2018-11-13	زیاد	آسیب‌پذیری‌های خرابی حافظه، اجرای کد از راه دور و افزایش سطح دسترسی در ویندوز به واسطه‌ی عدم مدیریت صحیح اشیاء در حافظه توسط موتور VBScript	برای ویندوز 10 1703 32, 64bit : goo.gl/q4hiKg برای ویندوزهای Server 2019 و 10 1809 32, 64bit : goo.gl/9XuY6D	goo.gl/RpfaiE
Windows	CVE-2018-8476	goo.gl/HxqtJe	2018-11-13	زیاد	آسیب‌پذیری اجرای کد از راه دور در ویندوز به واسطه‌ی عدم مدیریت صحیح اشیاء در حافظه توسط Windows Deployment Services TFTP Server	برای ویندوزهای 7 SP1 32, 64bit، Server 2008 R2 : goo.gl/hmmpcK برای ویندوزهای Server 2012 R2 و 8.1 32, 64bit : goo.gl/jirNmF	goo.gl/NTqhF7
Windows	CVE-2018-8454	goo.gl/cWMcpw	2018-11-13	متوسط	آسیب‌پذیری آشکارسازی اطلاعات حساس در ویندوز به واسطه‌ی عدم مدیریت صحیح اشیاء در حافظه توسط Windows Audio Service با اجرای یک برنامه‌ی کاربردی جعلی توسط یک مهاجم احراز هویت شده	برای ویندوزهای Server 2016 و 10 1803 32, 64bit : goo.gl/nB2AuR برای ویندوزهای Server 2016 و 10 1709 32, 64bit : goo.gl/66DCMi	goo.gl/QbisxD

Windows	CVE-2018-8416	goo.gl/RLjoVb	2018-11-13	متوسط	آسیب‌پذیری افزایش سطح دسترسی در ویندوز به واسطه‌ی مدیریت نامناسب فایل‌های جعلی خاص توسط هسته‌ی .NET. با ارسال یک فایل جعلی به سرور آسیب‌پذیر	برای .NET Core 2.1 : goo.gl/UmCo76	goo.gl/TK8A5F
Windows	CVE-2018-8415 CVE-2018-8256	goo.gl/XWAzHN goo.gl/JvYcDy	2018-11-13	متوسط	آسیب‌پذیری‌های اجرای کد از راه دور در ویندوز به واسطه‌ی وجود نقص در عملکرد PowerShell	برای ویندوزهای Server 2012 R2 و 8.1 32, 64bit : goo.gl/jirNmF برای ویندوزهای Server 2019 و 10 1809 32, 64bit : goo.gl/9XuY6D	goo.gl/SxyeUH goo.gl/VsB2rp
Windows	CVE-2018-8408	goo.gl/iQAt93	2018-11-13	متوسط	آسیب‌پذیری آشکارسازی اطلاعات حساس در ویندوز به واسطه‌ی مقداردهی نامناسب اشیاء در حافظه توسط هسته‌ی ویندوز با اجرای یک برنامه‌ی کاربردی جعلی روی سیستم قربانی توسط مهاجم احراز هویت شده	برای ویندوزهای 7 SP1 32, 64bit، Server 2008 R2 : goo.gl/hmmpcK برای ویندوزهای Server 2012 R2 و 8.1 32, 64bit : goo.gl/jirNmF	goo.gl/QipX6S

محیط‌های برنامه‌نویسی

دریافت آخرین نسخه‌ی پایدار

موضوع	آخرین نسخه پایدار	تاریخ عرضه	لینک دریافت
Joomla!	**3.9.0**	**2018-10-30**	**goo.gl/bWF9px**
Drupal	**8.6.3**	**2018-11-07**	**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-2018-17859 CVE-2018-17858 , …	goo.gl/FywkVH goo.gl/v6tkwc , …	2018-10-02	کم	چندین آسیب‌پذیری اجرای کد دلخواه، افزایش سطح دسترسی و غیره در Joomla! نسخه‌های ماقبل 3.8.13	آسیب‌پذیری فوق در Joomla! نسخه‌ی 3.8.13 برطرف شده است. goo.gl/bWF9px	goo.gl/mnZMdR goo.gl/q39y7j , …
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 و Server 2016 32, 64bit : 1803 goo.gl/hRMNKK	goo.gl/uUibvL
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 شده است. goo.gl/c5F8At	goo.gl/MkPF96

مرورگرهای اینترنت

دریافت آخرین نسخه‌ی پایدار

موضوع	آخرین نسخه پایدار	تاریخ عرضه	لینک دریافت
Mozilla Firefox	**63.0.3**	**2018-11-15**	**goo.gl/yIXtW**
Google Chrome	**70.0.3538.102**	**2018-11-09**	**goo.gl/Jk2diZ**

آسیب‌پذیری‌ها

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

Microsoft Edge	CVE-2018-8588 CVE-2018-8567 , …	goo.gl/jH1f8r goo.gl/Sisiqb , …	2018-11-13	زیاد	چندین آسیب‌پذیری اجرای کد از راه دور، افزایش سطح دسترسی، جعل و آشکارسازی اطلاعات حساس در مرورگر Microsoft Edge	برای ویندوزهای Server 2019 و 10 1809 32, 64bit : goo.gl/9XuY6D برای ویندوزهای Server 2016 و 10 1607 32 , 64bit : goo.gl/3WQjJg	goo.gl/1B7oU8 goo.gl/tRsSKT , …
Internet Explorer	CVE-2018-8570 CVE-2018-8552	goo.gl/JBcDwT goo.gl/J6km2u	2018-11-13	متوسط	آسیب‌پذیری‌های اجرای کد از راه دور، خرابی حافظه و افزایش سطح دسترسی در مرورگر Internet Explorer به واسطه‌ی دسترسی نامناسب به اشیاء در حافظه با ترغیب قربانی به باز کردن یک صفحه‌ی وب جعلی	برای Internet Explorer 11 روی ویندوزهای Server 2019 و 10 1809 32, 64bit : goo.gl/GjJ5vW	goo.gl/cvNct9 goo.gl/7HvYyv
Google Chrome	CVE-2018-6083 CVE-2018-6082 , …	goo.gl/4viXcG	2018-03-06	---	چندین آسیب‌پذیری دورزدن محدودیت‌های امنیتی، خرابی هیپ، افزایش سطح دسترسی، XSS، نشت اطلاعات، جلوگیری از سرویس و غیره در مرورگر Google Chrome با استفاده از یک صفحه‌ی HTML جعلی	آسیب‌پذیری فوق در مرورگر Google Chrome نسخه‌ی 65.0.3325.146 برطرف شده است. goo.gl/Jk2diZ	goo.gl/vdEGpf goo.gl/kqUjU6 , …

مجازی‌سازی

دریافت آخرین نسخه‌ی پایدار

موضوع	آخرین نسخه پایدار	تاریخ عرضه	لینک دریافت
VirtualBox	5.2.22	2018-11-09	goo.gl/l3wrf

آسیب‌پذیری‌ها

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

VMware ESXi, Workstation, Fusion	CVE-2018-6974	goo.gl/dQfJxc	2018-10-16	زیاد	آسیب‌پذیری اجرای کد در نسخه‌های مختلف VMware ESXi، Wokstation و Fusion به واسطه‌ی وجود نقص خواندن out-of-bounds در تجهیزات SVGA	آسیب‌پذیری فوق در ESXi نسخه‌های ESXi670-201810101-SG، ESXi650-201808401-BG، ESXi600-201808401-BG، Workstation نسخه‌ی 4.1.3 و Fusion نسخه‌ی 10.1.3 برطرف شده است.	goo.gl/pTFAuK
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

تجهیزات شبکه، دیواره‌های آتش و ضدبدافزار

موضوع	شناسه	منبع	تاریخ انتشار	سطح خطر	خلاصه‌ای از آسیب‌پذیری	نحوه رفع	اطلاعات بیشتر
Cisco ASA, FTD	CVE-2018-15454	goo.gl/XPKva7	2018-10-31	زیاد	آسیب‌پذیری جلوگیری از سرویس در Cisco ASA و Cisco FTD با نسخه‌ی نرم‌افزاری 9.9(2) به واسطه‌ی مدیریت نادرست ترافیک SIP توسط موتور نظارت SIP با ارسال درخواست‌های جعلی SIP	آسیب‌پذیری فوق در نسخه‌های نرم‌افزاری 9.10(1.1)، 9.9(2.31)، 100.13(0.192) و غیره برطرف شده است.	goo.gl/3M6SrJ
HPE iLO	CVE-2018-7105	goo.gl/bw8zQt	2018-10-22	----	آسیب‌پذیری‌های آشکارسازی اطلاعات و اجرای کد دلخواه در برخی نسخه‌های نرم‌افزاری HPE iLO 4، 5 HPE iLO و 3 HPE iLO	آسیب‌پذیری‌های فوق در HPE iLO 5 نسخه‌ی 1.35، HPE iLO 4 نسخه‌ی 2.61 و HPE iLO 3 نسخه‌ی 1.90 برطرف شده است. همچنین برای کاهش اثرات آسیب‌پذیری، اقداماتی نظیر غیرفعال کردن SSH و غیرفعال کردن پورت‌های سریال مؤثر است.	goo.gl/E1X4CT

ClamAV	CVE-2018-15378	goo.gl/QQHLW7	2018-10-03	----	آسیب‌پذیری جلوگیری از سرویس در ClamAV به واسطه‌ی بروز خطا در خواندن از حافظه در نتیجه‌ی نقص در عملکرد تابع unmew11() با استفاده از یک فایل اجرایی جعلی	آسیب‌پذیری فوق در ClamAV نسخه‌ی 0.100.2 برطرف شده است. goo.gl/9V44zY	goo.gl/2T2U84
NetApp	CVE-2018-5492	goo.gl/wJGCmQ	2018-10-03	زیاد	آسیب‌پذیری اجرای کد از راه دور در NetApp E-Series دارای نسخه‌های نرم‌افزاری مابین 11.30 الی 11.30.5	آسیب‌پذیری فوق در نسخه‌ی 11.30.5R1 برطرف شده است. goo.gl/oMU6kg	goo.gl/XUALiH
McAfee DLPe	CVE-2018-6689	goo.gl/2XoNt3	2018-10-02	زیاد	آسیب‌پذیری دورزدن محدودیت‌های امنیتی در McAfee Data Loss Prevention Endpoint به واسطه‌ی امکان دورزدن سازوکار احراز هویت	آسیب‌پذیری فوق در نسخه‌های 10.0.510 و 11.0.600 برطرف شده است.	goo.gl/SDnTsm
pfSense	CVE-2018-16055	goo.gl/GN6xNb	2018-08-28	----	آسیب‌پذیری‌های افزایش سطح دسترسی، اجرای دستور، خواندن فایل‌های دلخواه و غیره در pfsense به واسطه‌ی وجود نقص در عملکرد تابع dhcp_relinquish_lease()	آسیب‌پذیری فوق در pfsense نسخه‌ی 2.4.4 برطرف شده است. goo.gl/XEbXr9	goo.gl/tQ4Akg
Bitdefender	CVE-2017-8931	goo.gl/ST7qsX	2017-08-06	----	آسیب‌پذیری افزایش سطح دسترسی در Bitdefender GravityZone VMware appliance نسخه‌های ماقبل 6.2.1-35	آسیب‌پذیری فوق در نسخه‌ی 6.2.1-35 برطرف شده است.	goo.gl/BBozxb
Fortinet	CVE-2017-17541	goo.gl/2cqMNc	2018-07-05	----	آسیب‌پذیری تزریق کد جاوااسکریپت و HTML در Fortinet FortiManager 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 شده 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 12.1 RU6 و 14 RU1 MP1 برطرف شده است.	goo.gl/cbkCBG goo.gl/czaLYE

نرم‌افزارهای کاربردی

موضوع	شناسه	منبع	تاریخ انتشار	سطح خطر	خلاصه‌ای از آسیب‌پذیری	نحوه رفع	اطلاعات بیشتر
Microsoft Outlook	CVE-2018-8582 CVE-2018-8579 , …	goo.gl/YBLGXk goo.gl/15Xcsa , …	2018-11-13	متوسط	چندین آسیب‌پذیری اجرای کد از راه دور، آشکارسازی اطلاعات حساس و افزایش سطح دسترسی در Microsoft Outlook با ترغیب قربانی به باز کردن فایل پیوست rwz. در یک ایمیل جعلی	برای Microsoft Outlook 2016 64bit : goo.gl/2AWtWG برای Microsoft Outlook 2013 32bit : goo.gl/Kavqf3	goo.gl/1XCLh3 goo.gl/Yursy3 , …
Microsoft Dynamics 365	CVE-2018-8609 CVE-2018-8608 , …	goo.gl/8mB3eu goo.gl/11GNNS , …	2018-11-13	زیاد	چندین آسیب‌پذیری اجرای کد از راه دور و XSS در Microsoft Dynamics 365 نسخه‌ی 8 به واسطه‌ی عدم پاک‌سازی مناسب درخواست‌های وب	برای رفع آسیب‌پذیری‌های فوق، وصله‌ی زیر می‌بایست نصب گردد : goo.gl/8PscPF	goo.gl/pxSsn4 goo.gl/ooui6e , …
Microsoft Excel	CVE-2018-8577 CVE-2018-8574	goo.gl/H6XTrc goo.gl/HacCWP	2018-11-13	متوسط	آسیب‌پذیری اجرای کد از راه دور در Microsoft Excel به واسطه‌ی عدم مدیریت صحیح اشیاء در حافظه با استفاده از یک فایل جعلی Excel	برای Microsoft Excel 2016 64bit : goo.gl/Yso4eF برای Microsoft Office 2013 SP1 32bit : goo.gl/T6z5xa	goo.gl/4ahHEx goo.gl/JkRUsf
Microsoft Project	CVE-2018-8575	goo.gl/Yxd7vd	2018-11-13	متوسط	آسیب‌پذیری اجرای کد از راه دور و افزایش سطح دسترسی در Microsoft Project به واسطه‌ی عدم مدیریت صحیح اشیاء در حافظه با ترغیب قربانی به باز کردن یک فایل جعلی با این نرم‌افزار	برای Microsoft Project 2010 SP2 64bit : goo.gl/yWMt86 برای Microsoft Project 2016 32bit : goo.gl/aktgxZ	goo.gl/vc1hrT

Microsoft Word	CVE-2018-8573 CVE-2018-8539	goo.gl/VGJ6gD goo.gl/7CYckn	2018-11-13	متوسط	آسیب‌پذیری اجرای کد از راه دور و افزایش سطح دسترسی در Microsoft Word به واسطه‌ی عدم مدیریت صحیح اشیاء در حافظه با ترغیب قربانی به باز کردن یک فایل جعلی	برای Microsoft Word 2016 : 64bit goo.gl/AhoUYG برای Microsoft Office 2013 : SP2 32bit goo.gl/jz4RWM	goo.gl/92Hq84 goo.gl/zcGRPB
OpenSSL	CVE-2018-0734 CVE-2018-0735	goo.gl/ESnYtT goo.gl/Jsw2WV	2018-10-30	----	آسیب‌پذیری برگرداندن کلید خصوصی در OpenSSL به واسطه‌ی وجود timing side channel attack در الگوریتم‌های DSA و ECDSA	آسیب‌پذیری فوق در نسخه‌های 1.1.1a-dev، 1.1.0j-dev و 1.0.2q-dev برطرف شده است. goo.gl/nF79b8	goo.gl/2sBqPq goo.gl/A5FNhc
PRTG Network Monitor	CVE-2018-19204 CVE-2018-19203	goo.gl/qBkwbq goo.gl/gSkxmc	2018-10-25	زیاد	آسیب‌پذیری‌های اجرای کد دلخواه و جلوگیری از سرویس در PRTG Network Monitor با استفاده از یک درخواست HTTP جعلی	آسیب‌پذیری‌های فوق در PRTG Network Monitor نسخه‌ی 18.3.44.2054 برطرف شده است.	goo.gl/d9QNtm goo.gl/CVtGfJ
Centos Web Panel	CVE-2018-18324 CVE-2018-18323 CVE-2018-18322	goo.gl/3RFjW2	2018-10-15	----	آسیب‌پذیری‌های XSS، پیمایش دایرکتوری و تزریق دستور در Centos Web Panel نسخه‌ی 0.9.8.480	تاکنون راه حلی برای رفع این آسیب‌پذیری ارائه نگردیده است.	goo.gl/sbKwJb goo.gl/ckH7B8 goo.gl/LiZzCY
Intel Graphics Drivers	CVE-2018-12154 CVE-2018-12153 CVE-2018-12152	goo.gl/PHbn5z	2018-10-09	زیاد	آسیب‌پذیری‌های جلوگیری از سرویس، اجرای کد WebGL دلخواه و افزایش سطح دسترسی در Intel Graphics Drivers	آسیب‌پذیری‌های فوق در Intel Graphics Drivers نسخه‌های 10.18.x.5056، 10.18.x.5057 و 20.19x.5058 برطرف شده است. goo.gl/gGoWRT	goo.gl/PX8SEj goo.gl/24xZT9 goo.gl/wMeZDd
Cisco Prime Infrastructure	CVE-2018-15433 CVE-2018-15432 CVE-2018-15379	goo.gl/gsGscA goo.gl/cM5bdk goo.gl/5ctncY	2018-10-03	متوسط	آسیب‌پذیری‌های آشکارسازی اطلاعات و اجرای کد در Cisco Prime Infrastructure به واسطه‌ی وجود نقص در عملکرد تابع Server Backup و سرویس‌دهنده‌ی وب	برای آسیب‌پذیری آشکارسازی اطلاعات در نتیجه‌ی نقص در عملکرد تابع Server Backup تاکنون راه حلی ارائه نشده است. آسیب‌پذیری اجرای کد در Cisco PI نسخه‌های 3.3.1 u2 و 3.4.1 برطرف شده است.	goo.gl/VjNs37 goo.gl/6MUsuk goo.gl/bXebKy

Adobe Acrobat, Reader	APSB18-30	goo.gl/DBXbc7	2018-10-01	زیاد	چندین آسیب‌پذیری آشکارسازی اطلاعات حساس، اجرای کد دلخواه و افزایش سطح دسترسی 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 2019.008.20071 و در Acrobat 2017 و Acrobat Reader 2017 نسخه‌ی Classic در نسخه‌ی 2017.011.30105 برطرف شده است. goo.gl/9E1Y6	goo.gl/JKxmCA goo.gl/bqiU2n , …
Splunk	CVE-2018-7432 CVE-2018-7431 , …	goo.gl/yXpGwr goo.gl/qcbNLJ	2018-09-28	----	چندین آسیب‌پذیری XSS، جلوگیری از سرویس و دسترسی به فایل‌های دلخواه در نسخه‌های مختلف Splunk Enterprise و Splunk Light	آسیب‌پذیری‌های فوق در Splunk Enterprise نسخه‌های 6.2.14، 6.3.10، 6.4.7 و 6.5.3 و در Splunk Light نسخه‌ی 6.6.0 برطرف شده است.	goo.gl/qfvS8L goo.gl/pT96W8 , …
Telegram Desktop	CVE-2018-17613	goo.gl/DcWfpX	2018-09-27	----	آسیب‌پذیری نشت اطلاعات در Telegram Desktop نسخه‌ی 1.3.16 alpha به واسطه‌ی ارسال گواهی‌نامه‌ها و داده‌های نرم‌افزار به صورت متن واضح بر روی SOCKS5 در صورت فعال بودن Use Proxy	این آسیب‌پذیری در آخرین نسخه‌های نرم‌افزار برطرف شده است. goo.gl/FYp1DD	goo.gl/X4TrFg
Asterisk	CVE-2018-17281	goo.gl/A84kGz	2018-09-21	----	آسیب‌پذیری جلوگیری از سرویس در Asterisk به واسطه‌ی وجود سرریزی استک در ماژول res_http_websocket.so با ارسال یک درخواست HTTP جعلی	آسیب‌پذیری فوق در Asterisk نسخه‌های 13.23.1، 14.7.8 و 15.6.1 برطرف شده است.	goo.gl/gfu9r7
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 18.1.5 2017 و ماقبل آن	آسیب‌پذیری‌های فوق در نسخه‌های 2017 18.1.6 و 2018 19.1.6 برطرف شده است.	goo.gl/y6G3rv goo.gl/xGPgnq