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	۲.٤.۳۳	۲۰۱۸-۰۳-۱۷	goo.gl/ySdR
Squid Proxy & Cache Server	۳.٥.۲۷	۲۰۱۷-۰۸-۱۹	goo.gl/ZCyZ٦f

آسیب‌پذیری‌ها

موضوع	شناسه	منبع	تاریخ انتشار	سطح خطر	خلاصه‌ای از آسیب‌پذیری	نحوه رفع	اطلاعات بیشتر
Apache HTTP Server	CVE-۲۰۱۸-۱۳۱۲ CVE-۲۰۱۸-۱۳۰۳ CVE-۲۰۱۸-۱۳۰۲ , …	goo.gl/hjt۳yG goo.gl/QvARhv goo.gl/ci۱PrQ , …	۲۰۱۸-۰۳-۲۶	----	چندین آسیب‌پذیری جلوگیری از سرویس و دورزدن محدودیت‌های امنیتی در سرویس‌دهنده‌ی Apache HTTP Server نسخه‌های ماقبل ۲.۴.۳۰	آسیب‌پذیری‌های فوق در Apache HTTP Server نسخه‌ی ۲.۴.۳۰ برطرف شده است. goo.gl/ySdR	goo.gl/EQ۶wav goo.gl/Z۶MMTY goo.gl/MDcCPJ , …
Microsoft Project Server, Microsoft SharePoint	CVE-۲۰۱۸-۰۹۴۴ CVE-۲۰۱۸-۰۹۱۶ CVE-۲۰۱۸-۰۹۱۵ , …	goo.gl/kLUUG۴ goo.gl/f۴owrz goo.gl/tREgzh , …	۲۰۱۸-۰۳-۱۳	متوسط	چندین آسیب‌پذیری افزایش سطح دسترسی در Microsoft Project Server ۲۰۱۳ SP۱ و Microsoft SharePoint Server ۲۰۱۶	برای Microsoft Project Server ۲۰۱۳ SP۱ : goo.gl/Ar۴gbT برای Microsoft SharePoint Server ۲۰۱۶ : goo.gl/۶dUpiJ	goo.gl/n۳Cp۵۴ goo.gl/zFnfYZ goo.gl/۹vpGCF , …

موضوع	شناسه	منبع	تاریخ انتشار	سطح خطر	خلاصه‌ای از آسیب‌پذیری	نحوه رفع	اطلاعات بیشتر
Microsoft Exchange Server	CVE-۲۰۱۸-۰۹۴۱ CVE-۲۰۱۸-۰۹۴۰ CVE-۲۰۱۸-۰۹۲۴	goo.gl/۵uvFjm goo.gl/cu۹i۴D goo.gl/۸an۴Ek	۲۰۱۸-۰۳-۱۳	متوسط	آسیب‌پذیری‌های آشکارسازی اطلاعات و افزایش سطح دسترسی در نسخه‌های مختلف Microsoft Exchange Server	برای Microsoft Exchange Server ۲۰۱۶ CU۷ : goo.gl/eKUCTA برای Microsoft Exchange Server ۲۰۱۳ SP۱ : goo.gl/B۶Ebmq	goo.gl/TyiyZu goo.gl/jq۵۸ec goo.gl/yQx۶bb
Hyper-V	CVE-۲۰۱۸-۰۸۸۸ CVE-۲۰۱۸-۰۸۸۵	goo.gl/QdQqZ۵ goo.gl/hyj۵HX	۲۰۱۸-۰۳-۱۳	متوسط	آسیب‌پذیری‌های آشکارسازی اطلاعات و جلوگیری از سرویس در Hyper-V به واسطه‌ی عدم اعتبارسنجی صحیح ورودی کاربر روی سیستم عامل میزبان	برای ویندوزهای ۶۴bit ,۳۲ ۸.۱ و Server ۲۰۱۲ R۲ : goo.gl/YEj۷e۶ برای ویندوزهای ۳۲, ۱۷۰۹ ۱۰ ۶۴bit و ۱۷۰۹ Server ۲۰۱۶ : goo.gl/bKr۵KH	goo.gl/YqYYH۸ goo.gl/PBsDUx
ASP.NET	CVE-۲۰۱۸-۰۷۸۷	goo.gl/TRLszt	۲۰۱۸-۰۳-۱۳	متوسط	آسیب‌پذیری افزایش سطح دسترسی در ASP.NET نسخه‌های ۲.۰.۰ و ۲.۰.۱ با استفاده از تزریق HTML دلخواه توسط مهاجم هنگام شکست برنامه‌ی کاربردی تحت وب در اعتبارسنجی درخواست‌های وب	آسیب‌پذیری فوق در ASP.NET نسخه‌های ۲.۰.۲ و جدیدتر از آن رفع شده است.	goo.gl/msWnj۵
NTP	CVE-۲۰۱۸-۷۱۸۵ CVE-۲۰۱۸-۷۱۸۴ CVE-۲۰۱۸-۷۱۸۲ CVE-۲۰۱۸-۷۱۷۰	goo.gl/iQ۹۲Wv goo.gl/deSwSf goo.gl/ZDcpsh goo.gl/۴grsGg	۲۰۱۸-۰۲-۲۷	متوسط	چند آسیب‌پذیری جلوگیری از سرویس در NTP نسخه‌های ماقبل ۴.۲.۸p۱۱ و نسخه‌های ۴.۳.x الی ماقبل ۴.۳.۹۲	آسیب‌پذیری‌های فوق در NTP نسخه‌ی ۴.۲.۸p۱۱ برطرف شده است. goo.gl/uKW۷P۹	goo.gl/BoLkqR goo.gl/۵۶T۶۱W goo.gl/۷ZW۸Ym goo.gl/MV۳۳We
Squid Proxy Cache	CVE-۲۰۱۸-۱۰۰۰۰۲۷ CVE-۲۰۱۸-۱۰۰۰۰۲۴	goo.gl/۸VkHq۹ goo.gl/Kf۷uhR	۲۰۱۸-۰۱-۱۹	متوسط	آسیب‌پذیری جلوگیری از سرویس در Squid Proxy Cache به واسطه‌ی ارجاع به NULL Pointer و مدیریت ناصحیح اشاره‌گرها	آسیب‌پذیری فوق در نسخه‌ی ۴.۰.۲۳ برطرف شده است. goo.gl/utfvVW	goo.gl/N۹ckC۷ goo.gl/KwbZ۹V

سیستم‌های عامل

Windows	CVE-۲۰۱۸-۰۹۲۶ CVE-۲۰۱۸-۰۹۰۴ CVE-۲۰۱۸-۰۹۰۱ , …	goo.gl/uVq۳vF goo.gl/HHLLa۸ goo.gl/Ya۵۸er , …	۲۰۱۸-۰۳-۱۳	متوسط	چندین آسیب‌پذیری افزایش سطح دسترسی، اجرای کد، دورزدن محدودیت‌های امنیتی و غیره در ویندوز به واسطه‌ی نقص در عملکرد هسته‌ی ویندوز	برای ویندوزهای ۳۲, ۱۷۰۹ ۱۰ ۶۴bit و ۱۷۰۹ Server ۲۰۱۶ : goo.gl/bKr۵KH برای ویندوزهای ۶۴bit ,۳۲ ۸.۱ و Server ۲۰۱۲ R۲ : goo.gl/YEj۷e۶	goo.gl/ro۵QPz goo.gl/Dvo۷Ej goo.gl/JXWoFw , …
Windows	CVE-۲۰۱۸-۰۸۸۴	goo.gl/TFzWKa	۲۰۱۸-۰۳-۱۳	متوسط	آسیب‌پذیری دورزدن محدودیت‌های امنیتی در ویندوز به واسطه‌ی وجود نقص در عملکرد Windows Scripting Host (WSH) با اجرای یک برنامه‌ی مخرب توسط مهاجم روی سیستم قربانی	برای ویندوز ۶۴bit ,۳۲ ۱۷۰۳ ۱۰ : goo.gl/iMQe۷X برای ویندوز ۶۴bit ,۳۲ ۱۵۱۱ ۱۰ : goo.gl/GmZh۳۸	goo.gl/۱hXJz۷
Windows	CVE-۲۰۱۸-۰۸۸۳	goo.gl/tvDuCN	۲۰۱۸-۰۳-۱۳	متوسط	آسیب‌پذیری اجرای کد از راه دور در ویندوز به واسطه‌ی نقص در عملکرد Windows Shell هنگام اعتبارسنجی مسیر فایل کپی شده	برای ویندوزهای ۶۴bit ,۳۲ ۷ و Server ۲۰۰۸ R۲ : goo.gl/۴wvzcY برای ویندوزهای ۶۴bit ,۳۲ ۸.۱ و Server ۲۰۱۲ R۲ : goo.gl/YEj۷e۶	goo.gl/۴m۶nSD
Windows	CVE-۲۰۱۸-۰۸۸۲ CVE-۲۰۱۸-۰۸۸۰ CVE-۲۰۱۸-۰۸۷۷	goo.gl/SvAX۸o goo.gl/ovFXGF goo.gl/aATQax	۲۰۱۸-۰۳-۱۳	متوسط	چندین آسیب‌پذیری اجرای کد و افزایش سطح دسترسی در ویندوز به واسطه‌ی وجود نقص در عملکرد Desktop Bridge	برای ویندوزهای ۳۲, ۱۶۰۷ ۱۰ ۶۴bit و ۲۰۱۶ ۶۴bit Server : goo.gl/۳۲ZdAP برای ویندوزهای ۳۲, ۱۷۰۹ ۱۰ ۶۴bit و ۱۷۰۹ Server ۲۰۱۶ : goo.gl/bKr۵KH	goo.gl/yWXFhG goo.gl/zvvC۵N goo.gl/Ud۲۴Th
Windows	CVE-۲۰۱۸-۰۸۸۱	goo.gl/yG۲۴Ky	۲۰۱۸-۰۳-۱۳	متوسط	آسیب‌پذیری افزایش سطح دسترسی و اجرای کد در ویندوز به واسطه‌ی مدیریت نادرست اشیاء در حافظه توسط Microsoft Video Control	برای ویندوزهای ۶۴bit ,۳۲ ۸.۱ و Server ۲۰۱۲ R۲ : goo.gl/YEj۷e۶	goo.gl/HHxnXx

Windows	CVE-۲۰۱۸-۰۸۷۸	goo.gl/۹Cza۱۹	۲۰۱۸-۰۳-۱۳	متوسط	آسیب‌پذیری آشکارسازی اطلاعات در ویندوز به واسطه‌ی وجود نقص در Windows Remote Assistance هنگام پردازش XXE با ارسال یک فایل دعوت Remote Assistance جعلی	برای ویندوزهای ۶۴bit ,۳۲ ۷ و Server ۲۰۰۸ R۲ : goo.gl/۴wvzcY برای ویندوزهای ۶۴bit ,۳۲ ۸.۱ و Server ۲۰۱۲ R۲ : goo.gl/YEj۷e۶	goo.gl/xm۳۴Ma
Windows	CVE-۲۰۱۸-۰۸۶۸	goo.gl/J۵MxVd	۲۰۱۸-۰۳-۱۳	متوسط	آسیب‌پذیری اجرای کد و افزایش سطح دسترسی در ویندوز به واسطه‌ی عدم پاک‌سازی صحیح ورودی توسط Windows Installer	برای ویندوزهای ,۳۲ ۱۰ ۱۷۰۹ ۶۴bit و Server ۲۰۱۶ ۱۷۰۹ (Core Installation) : goo.gl/y۲cip۶	goo.gl/cP۶ftv
Windows	CVE-۲۰۱۸-۰۸۱۷ CVE-۲۰۱۸-۰۸۱۶ CVE-۲۰۱۸-۰۸۱۵	goo.gl/gboSof goo.gl/o۴hm۶h goo.gl/Dc۷Z۹D	۲۰۱۸-۰۳-۱۳	متوسط	چند آسیب‌پذیری افزایش سطح دسترسی و اجرای کد در ویندوز به واسطه‌ی مدیریت ناصحیح اشیاء در حافظه توسط Windows GDI	برای ویندوز ,۳۲ Server ۲۰۰۸ ۶۴bit : goo.gl/KbT۴SR برای ویندوزهای ۶۴bit ,۳۲ ۷ و Server ۲۰۰۸ R۲ : goo.gl/۴wvzcY	goo.gl/j۶ZZcF goo.gl/skA۴t۹ goo.gl/۸NjLR۲
Apple iTunes, iOS, iCloud, macOS, Safari, tvOS, watchOS	CVE-۲۰۱۷-۷۱۶۳ CVE-۲۰۱۷-۷۱۶۲ , …	goo.gl/ZGqRSP goo.gl/xY۵P۹p , …	۲۰۱۷-۱۲-۰۶	----	آسیب‌پذیری‌های دورزدن محدودیت‌های امنیتی، افزایش سطح دسترسی، اجرای کد از راه دور و جلوگیری از سرویس در محصولات Apple	این آسیب‌پذیری‌ها در iTunes نسخه‌ی ۱۲.۷.۲، iOS نسخه‌ی ۱۱.۲، macOS نسخه‌ی ۱۰.۱۳.۲، tvOS نسخه‌ی ۱۱.۲، watchOS نسخه‌ی ۴.۲، iCloud نسخه‌ی ۷.۲ و Safari نسخه‌ی ۱۱.۰.۲ برطرف شده است.	goo.gl/WfdgtY goo.gl/A۲N۸wi , …

محیط‌های برنامه‌نویسی

دریافت آخرین نسخه‌ی پایدار

موضوع	آخرین نسخه پایدار	تاریخ عرضه	لینک دریافت
Joomla!	**۳.۸.۶**	**۲۰۱۸-۰۳-۱۳**	**goo.gl/bWF۹px**

Drupal	**۸.۵.۱**	**۲۰۱۸-۰۳-۲۸**	**goo.gl/c۵F۸At**
WordPress	**٤.۹.٥**	**۲۰۱۸-۰٤-۰۳**	**goo.gl/DK۰Wx**

آسیب‌پذیری‌ها

موضوع	شناسه	منبع	تاریخ انتشار	سطح خطر	خلاصه‌ای از آسیب‌پذیری	نحوه رفع	اطلاعات بیشتر
Drupal	CVE-۲۰۱۸-۷۶۰۰	goo.gl/o۶vBdC	۲۰۱۸-۰۳-۲۸	زیاد	آسیب‌پذیری اجرای کد از راه دور در سیستم مدیریت محتوای Drupal نسخه‌های ماقبل ۸.۵.۱ و ۷.۵۸	آسیب‌پذیری فوق در Drupal نسخه‌های ۸.۵.۱ و ۷.۵۸ برطرف شده است. goo.gl/c۵F۸At	goo.gl/۵QD۵۳۴
Yii Framework	CVE-۲۰۱۸-۸۰۷۴ CVE-۲۰۱۸-۸۰۷۳ CVE-۲۰۱۸-۷۲۶۹	goo.gl/ZPd۲GV	۲۰۱۸-۰۳-۲۰	----	آسیب‌پذیری‌های اجرای کد و تزریق SQL در Yii Framework نسخه‌های ۲.x الی ماقبل ۲.۰.۱۵	آسیب‌پذیری‌های فوق در Yii Framework نسخه‌های ۲.۰.۱۵ برطرف شده است.	goo.gl/HDEkfY goo.gl/HoXba۷ goo.gl/۸FAVHb
Joomla!	CVE-۲۰۱۸-۸۰۴۵	goo.gl/Eyp۶RH	۲۰۱۸-۰۳-۱۲	کم	آسیب‌پذیری تزریق SQL در سیستم مدیریت محتوای Joomla! نسخه‌های مابین ۳.۵.۰ الی ۳.۸.۵	آسیب‌پذیری فوق در Joomla! نسخه‌ی ۳.۸.۶ برطرف شده است. goo.gl/bWF۹px	goo.gl/MKpMhV
.NET Framework	CVE-۲۰۱۸-۰۷۸۶ CVE-۲۰۱۸-۰۷۸۴	goo.gl/Egnn۸t goo.gl/ar۴oqs	۲۰۱۸-۰۱-۲۵	متوسط	آسیب‌پذیری‌های دورزدن محدودیت‌های امنیتی و جلوگیری از سرویس در .NET Framework و .NET Core. به واسطه‌ی عدم اعتبارسنجی صحیح گواهی‌نامه و عدم پردازش صحیح فایل‌های XML	برای .NET Framework نسخه‌های ۳.۵، ۴.۵.۲، ۴.۶، ۴.۶.۱، ۴.۶.۲، ۴.۷ و ۴.۷.۱ روی ویندوزهای ۸.۱ و سرور ۲۰۱۲ R۲ goo.gl/YwqF۶g	goo.gl/U۴n۴xX goo.gl/gdLN۱p

ASP.NET	CVE-۲۰۱۸-۰۷۸۵ CVE-۲۰۱۸-۰۷۸۴	goo.gl/HS۶ttm goo.gl/Me۲YRd	۲۰۱۸-۰۱-۰۹	متوسط	آسیب‌پذیری‌های CSRF و افزایش سطح دسترسی در ASP.NET Core ۲.۰	آسیب‌پذیری‌های فوق در نسخه‌ی ۲.۱.۴ برطرف شده است. goo.gl/yR۲XcZ goo.gl/pgV۵ZV	goo.gl/qJQ۱tK goo.gl/fNYhqo

مرورگرهای اینترنت

دریافت آخرین نسخه‌ی پایدار

موضوع	آخرین نسخه پایدار	تاریخ عرضه	لینک دریافت
Mozilla Firefox	**۵۹.۰.۲**	**۲۰۱۸-۰۳-۲۶**	**goo.gl/yIXtW**
Google Chrome	**۶۵.۰.۳۳۲۵.۱۸۱**	**۲۰۱۸-۰۳-۲۰**	**goo.gl/Jk۲diZ**

آسیب‌پذیری‌ها

موضوع	شناسه	منبع	تاریخ انتشار	سطح خطر	خلاصه‌ای از آسیب‌پذیری	نحوه رفع	اطلاعات بیشتر
Internet Explorer	CVE-۲۰۱۸-۰۹۴۲ CVE-۲۰۱۸-۰۹۳۵ CVE-۲۰۱۸-۰۹۲۹ , …	goo.gl/ezcQEj goo.gl/nJRuRq goo.gl/۸bc۶Rz , …	۲۰۱۸-۰۳-۱۳	متوسط	چندین آسیب‌پذیری آشکارسازی اطلاعات، اجرای کد، افزایش سطح دسترسی، جلوگیری از سرویس و غیره در مرورگر Internet Explorer	برای مرورگر Internet Explorer نسخه‌ی ۱۱ : روی ویندوزهای ۶۴bit ,۳۲ ۱۷۰۹ ۱۰ و Server ۲۰۱۶ ۱۷۰۹ ۶۴bit : goo.gl/Z۸۵DRP روی ویندوز ۶۴bit ,۳۲ ۱۷۰۳ ۱۰ : goo.gl/i۶HE۷X	goo.gl/۲rBf۲d goo.gl/rUX۲U۳ goo.gl/mdvjfW , …
Microsoft Edge	CVE-۲۰۱۸-۰۹۳۹ CVE-۲۰۱۸-۰۹۳۲ CVE-۲۰۱۸-۰۹۳۰ , …	goo.gl/PBHZs۹ goo.gl/om۶K۵P goo.gl/wa۲VoZ , …	۲۰۱۸-۰۳-۱۳	زیاد	چندین آسیب‌پذیری اجرای کد، افزایش سطح دسترسی و جلوگیری از سرویس در مرورگر Microsoft Edge	برای ویندوز ۶۴bit ,۳۲ ۱۷۰۳ ۱۰ : goo.gl/mzJ۷۸۲ برای ویندوزهای ۳۲, ۱۷۰۹ ۱۰ و Server ۲۰۱۶ ۱۷۰۹ ۶۴bit : goo.gl/Z۸۵DRP	goo.gl/Q۴vvB۳ goo.gl/aoC۲Tx goo.gl/۲yRArX , …

Google Chrome	CVE-۲۰۱۷-۵۱۳۳ CVE-۲۰۱۷-۵۱۳۲ CVE-۲۰۱۷-۵۱۳۱ , ...	goo.gl/dDTurt	۲۰۱۷-۱۰-۱۷	زیاد	چندین آسیب‌پذیری اجرای کد دلخواه، UXSS، دورزدن محدودیت‌های امنیتی، خرابی هیپ، جلوگیری از سرویس و غیره در مرورگر Google Chrome در ویندوز، لینوکس و مک	آسیب‌پذیری‌های فوق در مرورگر Google Chrome نسخه‌ی ۶۲.۰.۳۲۰۲.۶۲ برطرف شده است. goo.gl/Jk۲diZ	goo.gl/X۳EV۵B goo.gl/xKxVub goo.gl/eqUE۸e , ...

مجازی‌سازی

دریافت آخرین نسخه‌ی پایدار

موضوع	آخرین نسخه پایدار	تاریخ عرضه	لینک دریافت
VirtualBox	**۵.۲.۸**	**۲۰۱۸-۰۲-۲۷**	**goo.gl/l۳wrf**

آسیب‌پذیری‌ها

موضوع	شناسه	منبع	تاریخ انتشار	سطح خطر	خلاصه‌ای از آسیب‌پذیری	نحوه رفع	اطلاعات بیشتر
VMware Workstation, Fusion	CVE-۲۰۱۸-۶۹۵۷	goo.gl/GEZc۹e	۲۰۱۸-۰۳-۱۵	متوسط	آسیب‌پذیری جلوگیری از سرویس در نسخه‌های مختلف VMware Workstation و VMware Fusion در صورت باز کردن تعداد زیادی نشست VNC	آسیب‌پذیری فوق در VMware Workstation نسخه‌ی ۱۴.۱.۱ و VMware Fusion نسخه‌ی ۱۰.۱.۱ برطرف شده است.	goo.gl/۴w۴R۱G
Xen	CVE-۲۰۱۸-۷۵۴۲ CVE-۲۰۱۸-۷۵۴۱ CVE-۲۰۱۸-۷۵۴۰	goo.gl/۳NjSo۴ goo.gl/۴vc۳Qm goo.gl/TyF۳Me	۲۰۱۸-۰۳-۰۱	متوسط	چند آسیب‌پذیری جلوگیری از سرویس در نسخه‌های مختلف Xen (توقف سرویس‌دهی Hypervisor)	وصله‌های منتشر شده برای Xen نسخه‌های ۴.۱۰.x : goo.gl/QASL۹q goo.gl/Qit۱Qk goo.gl/qjjBUU goo.gl/AyGt۲g goo.gl/SnW۵BV goo.gl/WHGPyt goo.gl/LKUaNs goo.gl/A۵gebU goo.gl/۱Sa۳bv	goo.gl/h۶vbQD goo.gl/NWUgDz goo.gl/TvBQbc

VMware vCenter Server	CVE-۲۰۱۷-۴۹۲۸ CVE-۲۰۱۷-۴۹۲۷	goo.gl/FVYdht	۲۰۱۷-۱۱-۰۹	زیاد	آسیب‌پذیری‌های جلوگیری از سرویس، SSRF و CRLF در VMware vCenter Server	آسیب‌پذیری‌های فوق در VMware vCenter Server نسخه های ۶.۵ U۱، U۳c، ۶.۰ و U۳f ۵.۵ برطرف شده است.	goo.gl/wi۹۵mU goo.gl/MA۵Y۶t

تجهیزات شبکه، دیواره‌های آتش و ضدبدافزار

موضوع	شناسه	منبع	تاریخ انتشار	سطح خطر	خلاصه‌ای از آسیب‌پذیری	نحوه رفع	اطلاعات بیشتر
Cisco IOS, IOS XE	CVE-۲۰۱۸-۰۱۷۱	goo.gl/ct۵۷ez	۲۰۱۸-۰۴-۰۶	زیاد	آسیب‌پذیری اجرای کد از راه دور و جلوگیری از سرویس در برخی محصولات Cisco به دلیل وجود نقص در ویژگی Smart Install با ارسال داده‌های جعلی به پورت ۴۷۸۶ TCP تجهیز آسیب‌پذیر و وقوع شرایط سرریزی بافر	آسیب‌پذیری فوق در نسخه‌های نرم‌افزاری ۱۵.۲(۶)E۱، (۵.۷۲)۱۶.۳، ۱۵.۲(۲)E۸ و غیره برطرف شده است. همچنین می‌توان با زدن دستور no vstack و یا بستن پورت TCP ۴۷۸۶ از سوءاستفاده‌های احتمالی جلوگیری نمود.	goo.gl/rLqAo۴
Cisco IOS XE	CVE-۲۰۱۸-۰۱۵۰	goo.gl/NqaMmT	۲۰۱۸-۰۳-۲۸	زیاد	آسیب‌پذیری افزایش سطح دسترسی در برخی محصولات Cisco با نسخه‌ی IOS XE ۱۶.x نظیر ۱۶.۵.۱ (ورود به تجهیز آسیب‌پذیر با نام کاربری و کلمه‌ی عبور پیش‌فرض)	آسیب‌پذیری فوق در نسخه‌های نرم‌افزاری ۱۶.۶.۱، ۱۶.۶.۱a، ۱۶.۵.۲ و غیره برطرف شده است.	goo.gl/JVDVu۶
Cisco IOS, IOS XE	CVE-۲۰۱۸-۰۱۵۹	goo.gl/TM۴۳kx	۲۰۱۸-۰۳-۲۸	زیاد	آسیب‌پذیری جلوگیری از سرویس در برخی محصولات Cisco به واسطه‌ی نقص در پیاده‌سازی IKEv۱ با ارسال بسته‌های جعلی IKEv۱	آسیب‌پذیری فوق در نسخه‌های نرم‌افزاری ۱۵.۴(۲)S۱، ۱۵.۴(۲)T۱ و غیره برطرف شده است.	goo.gl/k۳toZd
ClamAV	CVE-۲۰۱۸-۰۲۰۲	goo.gl/tYFexb goo.gl/x۸VLbK	۲۰۱۸-۰۳-۰۸	----	آسیب‌پذیری جلوگیری از سرویس در ClamAV نسخه‌های ماقبل ۰.۹۹.۴ به واسطه‌ی سازوکار اعتبارسنجی نامناسب ورودی هنگام پردازش و مدیریت فایل‌های PDF	برای رفع آسیب‌پذیری فوق روی Ubuntu برای نسخه‌های مختلف : goo.gl/jKfy۴a goo.gl/jBYWE۸ goo.gl/xR۵zHb	goo.gl/XW۳Nwq

موضوع	شناسه	منبع	تاریخ انتشار	سطح خطر	خلاصه‌ای از آسیب‌پذیری	نحوه رفع	اطلاعات بیشتر
BitDefender Total Security ۲۰۱۸	CVE-۲۰۱۸-۶۱۸۳	goo.gl/m۸gyHB	۲۰۱۸-۰۳-۰۶	----	آسیب‌پذیری افزایش سطح دسترسی در BitDefender Total Security ۲۰۱۸	تاکنون راه حلی برای رفع این آسیب‌پذیری ارائه نشده است.	goo.gl/Ci۵h۳v
Suricata	CVE-۲۰۱۸-۶۷۹۴	goo.gl/n۳heS۳	۲۰۱۸-۰۳-۰۶	متوسط	آسیب‌پذیری دورزدن محدودیت‌های امنیتی در Suricata با ارسال داده قبل از اتمام مراحل دست‌تکانی سه مرحله‌ای توسط مهاجم	آسیب‌پذیری فوق در Suricata نسخه‌ی ۴.۰.۴ برطرف شده است. goo.gl/Ytg۳pf	goo.gl/pB۶zFM
Fortinet FortiGate	CVE-۲۰۱۲-۰۹۴۱	goo.gl/AFmfxq	۲۰۱۲-۰۱-۳۱	متوسط	آسیب‌پذیری آشکارسازی اطلاعات در Fortinet FortiGate نسخه‌های نرم‌افزاری ۴.۳ الی ۴.۳.۵	آسیب‌پذیری فوق در نسخه‌ی نرم‌افزاری ۴.۳.۶ برطرف شده است.	goo.gl/rscGA۳
pfSense	CVE-۲۰۱۷-۱۰۰۰۴۷۹	goo.gl/Q۵sWKv	۲۰۱۸-۰۱-۰۵	متوسط	آسیب‌پذیری اجرای کد و افزایش سطح دسترسی در دیواره‌ی آتش pfSense به واسطه‌ی وجود CSRF	آسیب‌پذیری فوق در pfSense نسخه‌ی ۲.۴.۲-RELEASE برطرف شده است. goo.gl/MSmRFh	goo.gl/exg۷vB
Mikrotik RouterOS	CVE-۲۰۱۷-۱۷۵۳۸ CVE-۲۰۱۷-۱۷۵۳۷	goo.gl/۹ADy۶V goo.gl/Lu۸۳۴f	۲۰۱۷-۱۲-۱۳	زیاد	آسیب‌پذیری جلوگیری از سرویس در Mikrotik RouterOS نسخه‌های ۶.۴۰.۵ و ۶.۳۹.۲ با استفاده از ارسال چندین کاراکتر \۰ پس از اتصال به پورت ۵۳ و یا ارسال سیل‌آسای بسته‌های ICMP	تاکنون راه حلی برای رفع این آسیب‌پذیری ارائه نشده است.	goo.gl/LxR۴kB goo.gl/DobKff

نرم‌افزارهای کاربردی

Adobe Flash Player	APSB۱۸-۰۵	goo.gl/Lcaqw۷	۲۰۱۸-۰۳-۱۳	زیاد	آسیب‌پذیری اجرای کد از راه دور در Adobe Flash Player در سیستم‌های عامل ویندوز، لینوکس، مک و Chrome OS	این آسیب‌پذیری‌ها در Adobe Flash Player نسخه‌ی ۲۹.۰.۰.۱۱۳ در ویندوز، مک، لینوکس و Chrome OS برطرف شده است. goo.gl/qDW۹E مرورگرهای Internet Explorer، Microsoft Edge و Google Chrome را به‌روزرسانی کنید. ویندوزهای ۸.۱ و ۱۰ را به‌روزرسانی نمائید.	goo.gl/Lcaqw۷
Adobe Dreamweaver CC	APSB۱۸-۰۷	goo.gl/j۸umNi	۲۰۱۸-۰۳-۱۳	زیاد	آسیب‌پذیری اجرای کد دلخواه در Adobe Dreamweaver CC نسخه‌های ۱۸.۰ و ماقبل آن در ویندوز	آسیب‌پذیری فوق در Adobe Dreamweaver CC نسخه‌ی ۱۸.۱ برطرف شده است.	goo.gl/j۸umNi
Microsoft Office	CVE-۲۰۱۸-۰۹۲۲ CVE-۲۰۱۸-۰۹۱۹ CVE-۲۰۱۸-۰۹۰۷	goo.gl/kzjVYY goo.gl/WE۶Zwt goo.gl/VFZE۱E , …	۲۰۱۸-۰۳-۱۳	متوسط	چندین آسیب‌پذیری اجرای کد از راه دور، آشکارسازی اطلاعات، دورزدن محدودیت‌های امنیتی و غیره در Microsoft Office	برای Microsoft Office ۲۰۱۰ : SP۲ ۳۲bit goo.gl/LCh۶d۴ برای Microsoft Office ۲۰۱۳ : SP۱ ۳۲bit goo.gl/fRHJbk	goo.gl/۸CeWPk goo.gl/UspzPn goo.gl/ZUiwoi , …
Asterisk	CVE-۲۰۱۸-۷۲۸۷ CVE-۲۰۱۸-۷۲۸۶ CVE-۲۰۱۸-۷۲۸۵ CVE-۲۰۱۸-۷۲۸۴	goo.gl/TihoSK goo.gl/FUBMJW goo.gl/BgTxnS goo.gl/WBDBv۷	۲۰۱۸-۰۲-۲۲	متوسط	چندین آسیب‌پذیری جلوگیری از سرویس در نسخه‌های مختلف Asterisk به واسطه‌ی وجود سرریزی بافر، NULL Pointer و غیره	آسیب‌پذیری‌های فوق در Asterisk نسخه‌های ۱۵.۲.۲، ۱۴.۷.۶ و ۱۳.۱۹.۲ برطرف شده است. goo.gl/yi۲۲NY	goo.gl/U۲LbYu goo.gl/LezZkM goo.gl/۵d۳oGH goo.gl/jrrC۳۱

Adobe Acrobat, Reader	APSB۱۸-۰۲	goo.gl/oHiA۸n	۲۰۱۸-۰۲-۱۳	زیاد	چندین آسیب‌پذیری افزایش سطح دسترسی و اجرای کد 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 نسخه‌های Continuous و Classic به ترتیب در نسخه‌های ۲۰۱۸.۰۱۱.۲۰۰۳۵ و ۲۰۱۵.۰۰۶.۳۰۴۱۳ و در ۲۰۱۷ Acrobat و Acrobat ۲۰۱۷ Reader نسخه‌ی ۲۰۱۷.۰۱۱.۳۰۰۷۸ برطرف شده است. goo.gl/۹E۱Y۶	goo.gl/oHiA۸n
Hotspot Shield	CVE-۲۰۱۸-۶۴۶۰	goo.gl/P۲BrDm	۲۰۱۸-۰۱-۳۰	زیاد	آسیب‌پذیری آشکارسازی اطلاعات در Hotspot Shield به واسطه‌ی عدم فیلترسازی مناسب ورودی‌های کاربر با ارسال یک درخواست POST با پارامتر func=$_APPLOG.Rfunc	تاکنون راه حلی برای رفع آسیب‌پذیری فوق ارائه نشده است.	goo.gl/eZbXAT
FreeNAS	CVE-۲۰۱۴-۵۳۳۴	goo.gl/Y۱S۲uF	۲۰۱۸-۰۱-۰۸	----	آسیب‌پذیری افزایش سطح دسترسی در FreeNAS به واسطه‌ی عدم وجود کلمه عبور روی کاربر Admin به صورت پیش‌فرض	آسیب‌پذیری فوق در FreeNAS نسخه ی ۹.۳-M۳ برطرف شده است. goo.gl/pXnhqb	goo.gl/FMqSZD
HP Printers	CVE-۲۰۱۷-۲۷۵۰ CVE-۲۰۱۷-۲۷۴۳	goo.gl/bupg۶P goo.gl/BbLhYw	۲۰۱۷-۱۲-۲۰	زیاد	آسیب‌پذیری‌های اجرای کد دلخواه و XSS در برخی محصولات HP از جمله HP LaserJet Enterprise printers، HP Enterprise LaserJet Printers and MFPs و غیره	برای رفع آسیب‌پذیری‌های فوق باید نسخه‌های نرم‌افزاری به‌روز گردد. goo.gl/w۵Cb۴J	goo.gl/t۹DuMz goo.gl/X۸NRt۳
WPA, WPA۲	CVE-۲۰۱۷-۱۳۰۸۸ CVE-۲۰۱۷-۱۳۰۸۷ CVE-۲۰۱۷-۱۳۰۸۶ , ...	goo.gl/۳pGKhB	۲۰۱۷-۱۰-۱۶	متوسط	چندین آسیب‌پذیری دسترسی به اطلاعات در استاندارد WPA و WPA۲ با استفاده از ترغیب قربانی به نصب مجدد کلید دست‌تکانی	برای رفع این آسیب‌پذیری تاکنون برای برخی از تجهیزاتی که این استاندارد در آن‌ها پیاده‌سازی شده است، راه حل‌هایی ارائه شده است.	goo.gl/gS۲euy goo.gl/ovMrdm goo.gl/AWddm۸ , ...