



نشرة

لعدد من الثغرات الحديثة المكتشفة مؤخرًا

إعداد

ماجد اسماعيل

دائرة الدراسات والأبحاث

آب-2020

ثغرات عالية مستوى الخطورة

apache – http_server Vulnerability CVE-2020-11984	اسم الثغرة
عالي	مستوى الخطورة
ثغرة في الوحدة mod_proxy_uwsgi، تسمح للمهاجمين بكشف معلومات هامة وقد تسمح لهم أيضاً بتنفيذ رمازات تعسفية عن بعد.	التوصيف والتأثير
Apache HTTP server 2.4.32 to 2.4.44	الإصدارات المتأثرة
httpd.apache.org/security/vulnerabilities_24.html	الحلول المقترحة وتفاصيل إضافية

apache – skywalking Vulnerability CVE-2020-13921	اسم الثغرة
عالي	مستوى الخطورة
ثغرة حقن رمازات بلغة الاستعلام البنوية SQL Injection في منصة الإدارة والمراقبة Apache SkyWalking H2/MySQL/TiDB، وذلك في حال استخدام إحدى التقنيات التالية كمنصات تخزينية:	التوصيف والتأثير
Apache SkyWalking 6.5.0, 6.6.0, 7.0.0, 8.0.0, 8.0.1	الإصدارات المتأثرة
https://lists.apache.org/thread.html/r6f3a934ebc54585d8468151a494c1919dc1ee2cccaf237ec434dbbd6@%3Cdev.skywalking.apache.org%3E	الحلول المقترحة وتفاصيل إضافية

php_factory – multiple_products Vulnerability CVE-2020-5616	اسم الثغرة
عالي	مستوى الخطورة
ثغرات متعددة في عدد من منتجات PHP Factory تسمح للمهاجمين بتجاوز إجراءات المصادقة والدخول بصلاحيات إدارية.	التوصيف والتأثير
[Calendar01] free edition ver1.0.0 [Calendar02] free edition ver1.0.0 [PKOBO-News01] free edition ver1.0.3 and earlier	الإصدارات المتأثرة

[PKOBO–vote01] free edition ver1.0.1 and earlier [Telop01] free edition ver1.0.0 [Gallery01] free edition ver1.0.3 and earlier [CalendarForm01] free edition ver1.0.3 and earlier [Link01] free edition ver1.0.0	
https://jvn.jp/en/jp/JVN73169744/index.html	الحلول المقترحة وتفاصيل إضافية

tp-link – tl-ps310u_devices Vulnerability CVE-2020-15055	اسم الثغرة
	مستوى الخطورة عالي
ثغرة في أحد المنتجات USB-Ethernet، تسمح للمهاجمين على نفس الشبكة بتجاوز إجراءات المصادقة وذلك من خلال الإدارة عبر الويب.	التوصيف والتأثير
TL-PS310U devices before 2.079.000.t0210	الإصدارات المتأثرة
https://research.hisolutions.com/2020/07/high-impact-vulnerabilites-in-multiple-usb-network-servers/	الحلول المقترحة وتفاصيل إضافية

vmware – kryo_codec Vulnerability CVE-2020-15055	اسم الثغرة
	مستوى الخطورة عالي
ثغرة في المكوّن kryo_codec والذي يوفره إطار العمل Spring Integration، تتواجد هذه الثغرة في حال إعداد المكوّن بالإعدادات الافتراضية وتزويد المكون ببيانات تحوي رمازات خبيثة أثناء عملية إلغاء تسلسل بعض الوحدات المضافة، بالنهاية قد يسمح الاستغلال الناجح لهذه الثغرة بتنفيذ رمازات تعسفية.	التوصيف والتأثير
Spring Integration 4.3.0 to 4.3.22 5.1.0 to 5.1.11 5.2.0 to 5.2.7 5.3.0 to 5.3.1	الإصدارات المتأثرة
https://tanzu.vmware.com/security/cve-2020-5413	الحلول المقترحة وتفاصيل إضافية

tp-link – tl-ps310u_devices Vulnerability CVE-2020-15055	اسم الثغرة
عالي	مستوى الخطورة
ثغرة في أحد أجهزة USB-Ethernet، تسمح للمهاجمين على نفس الشبكة بتجاوز إجراءات المصادقة وذلك من خلال الإدارة عبر الويب.	التوصيف والتأثير
TL-PS310U devices before 2.079.000.t0210	الإصدارات المتأثرة
https://research.hisolutions.com/2020/07/high-impact-vulnerabilites-in-multiple-usb-network-servers/	الحلول المقترحة وتفاصيل إضافية

ثغرات متوسطة مستوى الخطورة

apache -- http_server Vulnerability CVE-2020-11985	اسم الثغرة
متوسط	مستوى الخطورة
ثغرة انتحال العنوان الرقمي عند استخدام كل من الوحدات mod_rewrite، mod_remoteip حيث سيتمكن المهاجم من إجراء مصادقة غير مصرح بها بالإضافة إلى تنفيذ رمازات PHP وذلك بعد انتحاله لعنوان رقمي ما.	التوصيف والتأثير
Apache 2.4.23, 2.4.20, 2.4.18, 2.4.17, 2.4.16, 2.4.12, 2.4.10, 2.4.9, 2.4.7, 2.4.6, 2.4.4, 2.4.3, 2.4.2, 2.4.1	الإصدارات المتأثرة
https://httpd.apache.org/security/vulnerabilities_24.html	الحلول المقترحة وتفاصيل إضافية

apache -- http_server Vulnerability CVE-2020-11993	اسم الثغرة
متوسط	مستوى الخطورة
خطأ إجراء بيانات الدخول على اتصال غير صحيح، وذلك عند تفعيل وضعية التتبع والتصحيح trace/debug من أجل الوحدات العاملة بالبروتوكول HTTP/2	التوصيف والتأثير

Apache 2.4.43, 2.4.39, 2.4.38, 2.4.37, 2.4.35, 2.4.34, 2.4.33, 2.4.30, 2.4.29, 2.4.28, 2.4.27, 2.4.26, 2.4.25, 2.4.23, 2.4.20	الإصدارات المتأثرة
https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2020-11993	الحلول المقترحة وتفاصيل إضافية

bitdefender -- endpoint_security_for_mac Vulnerability CVE-2020-8108	اسم الثغرة
متوسط	مستوى الخطورة
ثغرة في عملية المصادقة تسمح لبعض الإجراءات غير المتمتعة بالصلاحيات المناسبة بإجراء إعادة إقلاع للخدمة الرئيسية وإمكانية حقن رمازات ضمن إجراءات موثوقة.	التوصيف والتأثير
Bitdefender Endpoint Security for Mac	الإصدارات المتأثرة
https://www.bitdefender.com/support/security-advisories/insufficient-client-validation-bitdefender-endpoint-security-mac-va-8759/	الحلول المقترحة وتفاصيل إضافية

huawei – fusioncomput Vulnerability CVE-2020-9248	اسم الثغرة
متوسط	مستوى الخطورة
ثغرة تفويض غير صحيح ناتجة عن عملية تحقق غير كافية من قبل الوحدة المعنية لبعض المدخلات، حيث يتم منح بعض الصلاحيات لبعض الملفات وذلك مع وصول غير صحيح.	التوصيف والتأثير
Huawei FusionComput 8.0.0	الإصدارات المتأثرة
https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200729-01-fc-en	الحلول المقترحة وتفاصيل إضافية

libx11 -- libx11 Vulnerability CVE-2020-14344	اسم الثغرة
متوسط	مستوى الخطورة
خطأ تجاوز سعة integer overflow يؤدي إلى خطأ تجاوز سعة heap-buffer overflow وذلك ضمن المنهجية X Input Method (XIM) client.	التوصيف والتأثير

libX11 before version 1.6.10	الإصدارات المتأثرة
https://nvd.nist.gov/vuln/detail/CVE-2020-14344	الحلول المقترحة وتفاصيل إضافية

linux – etcd Vulnerability CVE-2020-15115	اسم الثغرة
متوسط	مستوى الخطورة
تعاني بعض إصدارات تقنية etcd من مشكلة عدم التحقق من الطول الفعلي لكلمات المرور، مما يسمح باستخدام كلمات مرور قصيرة حتى تلك التي تحوي حرفاً واحداً، قد يسمح هذا للمهاجمين بتخمين كلمات المرور أو إطلاق هجمات brute-force.	التوصيف والتأثير
etcd before versions 3.3.23 and 3.4.10	الإصدارات المتأثرة
https://github.com/etcd-io/etcd/security/advisories/GHSA-4993-m7g5-r9hh	الحلول المقترحة وتفاصيل إضافية

Plesk – obsidian Vulnerability CVE-2020-11583	اسم الثغرة
متوسط	مستوى الخطورة
ثغرة حقن رمازات عبر الموقع XSS Reflected تسمح للمهاجمين غير المرخصين بحقن رمازات تعسفية من نوع JavaScript, HTML, or CSS ويتم ذلك باستخدام المنهجية GET	التوصيف والتأثير
Plesk Obsidian 18.0.17	الإصدارات المتأثرة
https://nvd.nist.gov/vuln/detail/CVE-2020-11583	الحلول المقترحة وتفاصيل إضافية

plesk – onyx Vulnerability CVE-2020-11584	اسم الثغرة
متوسط	مستوى الخطورة
ثغرة حقن رمازات عبر الموقع XSS Reflected تسمح للمهاجمين غير المرخصين بحقن رمازات تعسفية من نوع JavaScript, HTML, or CSS ويتم ذلك باستخدام المنهجية GET	التوصيف والتأثير
Plesk Onyx 17.8.11	الإصدارات المتأثرة

https://nvd.nist.gov/vuln/detail/CVE-2020-11584	الحلول المقترحة وتفاصيل إضافية
vmware – gemfire Vulnerability CVE-2020-5396	اسم الثغرة
	مستوى الخطورة
متوسط تحدث هذه الثغرة لدى تجهيز الأنظمة بدون استخدام تقنية SecurityManager مع وجود خدمة JMX، يؤدي هذا الوضع برمته إلى وجود إعدادات افتراضية غير آمنة، كل هذا سيسمح للمستخدمين بإطلاق هجمات تنفيذ رمازت عن بعد.	التوصيف والتأثير
VMware GemFire versions prior to 9.10.0, 9.9.2, 9.8.7, and 9.7.6, and VMware Tanzu GemFire for VMs versions prior to 1.11.1 and 1.10.2	الإصدارات المتأثرة
https://tanzu.vmware.com/security/cve-2020-5396	الحلول المقترحة وتفاصيل إضافية