شماره بیست و هفتم - فروردین ۱۳۹۷

خبرنامه "آپا" دانشگاه خوارزمی

KHARAZMI CERT
COORDINATION CENTER
مرکز تخصصی آپا خوارزمی

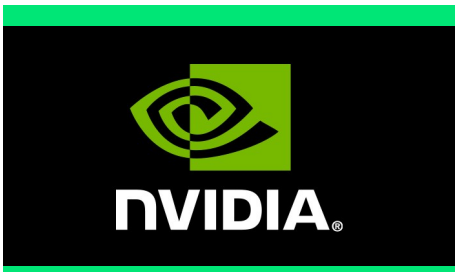
در این شماره خواهید خواند:

وصله امنیتی سیسکو برای دو مدل از مسیریاب‌هایش

سیسکو اعلام کرد که پچ‌های جدیدی را برای روترهای RV320و RV325منتشر کرده است تا به طور صحیح آسیب پذیری‌هایی را که برای حملاتی در طی دو ماه مورد هدف قرار گرفته بود، شناسایی کند. این شرکت تلاش کرد آسیب پذیری‌ها را در ماه ژانویه حل کند. - صفحه ۲

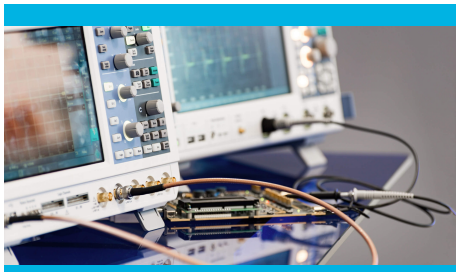
ضعف امنیتی جدید وب سرور آپاچی

در اول آپریل یکی از اعضای بنیانگذار بنیاد نرم افزار آپاچی و پروژه OpenSSL به نام Mark J Cox در توییتر خود هشداری در مورد یک نقص مهم در پروتکل Apache HTTP Server را ارسال کرد. وب سرور آپاچی یکی از محبوب ترین و گسترده ترین وب سرورهای منبع باز در جهان است که تقریبا ۴۰ درصد از کل اینترنت را پشتیبانی می کند. - صفحه ۳



وصله‌های امنیتی برای رفع آسیب پذیری‌های متعدد در NVIDIA

شرکت بزرگ تولید کننده‌ی کارت‌های گرافیک بسیار محبوب NVIDIA چند مدتی است که درگیر آسیب پذیری‌های شده است که بسیار بر نام و اعتبار این شرکت تاثیر گذاشته است. - صفحه ۴



روش جدید محققان برای کشف بدافزارهای پنهان در سخت افزارها

نرم افزارها همیشه قادر به کشف بدافزارهای موجود در فریمورهای سخت افزارها نیستند. تشخیص هک‌های سخت افزاری به شدت دشوار بوده اما پیشرفتی بزرگ در جلوگیری از این حملات به تازگی صورت گرفته است. - صفحه ۵

تبدیل شرکت‌های آسیایی را به یک ماینر Monero

تیم امنیت نرم افزار شرکت Symantec روز چهرشنبه خبری را در وبلگ خود انتشار داد که براساس آن، ۸۰ درصد از قربانیان این بدافزار در چین وبا ملیت کره جنوبی، ژاپن و ویتنام هستند. - صفحه ۶

نقص بحرانی روز صفر در سرور اوراکل WebLogic

محققان امنیتی یک نقص "بسیار بحرانی" روز صفر را در سرور اوراکل WebLogic کشف کرده اند که این نقص بر تمامی نسخه های WebLogic تاثیر می گذارد. آسیب پذیری اجازه می دهد تا هکرها بتوانند کد های دلخواه را از راه دور اجرا کنند. - صفحه ۷

وصله امنیتی سیسکو برای دو مدل از مسیریاب‌هایش

سیسکو اعلام کرد که پچ‌های جدیدی را برای روترهای RV320 و RV325 منتشر کرده است تا به طور صحیح آسیب پذیری‌هایی را که برای حملاتی در طی دو ماه مورد هدف قرار گرفته بود، شناسایی کند. این شرکت تلاش کرد آسیب پذیری‌ها را در ماه ژانویه حل کند، اما پچ‌هایی که در ابتدا منتشر شدند ناقص بودند. بیش از ۹،۶۰۰ روتر در معرض آسیب قرار گرفتند هر دو آسیب پذیری بر روی رابط مدیریتی مبتنی بر روترهای RV320 و RV325 تاثیر می گذارد. اولین آن‌ها به عنوان CVE-2019-1653 ردیابی می‌شود و می‌تواند به یک مهاجم ناشناس، از راه دور برای بازیابی اطلاعات حساس اجازه دهد. این مسئله ناشی از کنترل دسترسی نامناسب برای URL است. مهاجم می‌تواند با آسیب پذیری از طریق اتصال به یک دستگاه آسیب دیده از طریق HTTP یا HTTPS و درخواست URL خاص استفاده کند. یک درخواست URL خاص استفاده کند. یک سوءاستفاده موفق می‌تواند به مهاجم اجازه دهد پیکربندی روتر یا اطلاعات تشخیصی دقیق را دانلود کند این بهره برداری می‌تواند منجر به نقص دوم شود، که به عنوان CVE-2019-1652 ردیابی می‌شود و دلیل اعتبار نامعتبر ورودی کاربر است. این می‌تواند به یک مهاجم دارای مجوز معتبر با امتیازات اداری در یک دستگاه آسیب دیده برای اجرای دستورات دلخواه اجازه دهد. مهاجم می‌تواند از طریق ارسال درخواست-های HTTP POST مخرب به رابط مدیریتی مبتنی بر یک دستگاه آسیب دیده از این آسیب پذیری بهره برداری کند. یک سوءاستفاده موفق می‌تواند به مهاجم اجازه دهد دستورات دلخواه را بر روی پوسته لینوکس به عنوان root اجرا کند. هر دو این آسیب پذیری‌ها بر روترهای کوچک RV320 و RV325 پچ شده است.

گردآورنده: امیرحسین ضرغامی

ضعف امنیتی جدید وب سرور آپاچی

در اول آپریل یکی از اعضای بنیانگذار بنیاد نرم افزار آپاچی و پروژه OpenSSL به نام Mark J Cox در توییتر خود هشداری در مورد یک نقص مهم در پروتکل Apache HTTP Server را ارسال کرد. وب سرور آپاچی یکی از محبوب ترین و گسترده ترین وب سرورهای منبع باز در جهان است که تقریبا ۴۰ درصد از کل اینترنت را پشتیبانی می کند.

این آسیب پذیری که به نام CVE-2019-0211 شناسایی شده است و توسط توسعه دهندگان آپاچی در آخرین نسخه ۲.۴.۳۹ نرم افزار آن که در دوم آپریل منتشر شده، پچ شده است. این نقص در نسخه ۲.۴.۱۷ آپاچی HTTP Server از طریق ۲.۴.۳۸ تحت تاثیر قرار می‌گیرد و می‌تواند هر کاربر کمتری را مجاز به اجرای کد دلخواه با امتیازات ریشه در سرور هدف قرار دهد.

اگر چه هنوز یک کد اثبات (PoC) برای این نقص ارائه نشده است. این آسیب پذیری بیشتر مربوط به خدمات میزبانی وب است که در آن مشتریان مخرب یا هکرهایی که توانایی اجرای اسکریپت‌های PHP یا CGI را در یک وب سایت دارند می‌توانند از نقص دسترسی ریشه در سرور استفاده کنند و در نهایت به همه دیگران آسیب برسانند وب سایت های میزبانی شده در همان سرور. علاوه بر این، آخرین نسخه Apache HTTPD 2.4.39 همچنین دارای سه آسیب پذیری کم و دو آسیب پذیری مهم دیگر است. دومین خطای مهم (CVE-2019-0217) می تواند به کاربر اجازه می دهد تا با اعتبار معتبر برای احراز هویت با استفاده از نام کاربری دیگر، دور زدن محدودیت های کنترل پیکربندی دسترسی داشته باشد. سومین آسیب پذیری، مداخله کنترل دسترسی mod_ssl است (CVE-2019-0215)، یک خطا در mod_ssl هنگام استفاده از تأیید گواهی کلاینت هر مکان با TLSv1.3 اجازه داد که مشتری پشتیبانی از Post-Authentication Handshake را از محدودیت‌های کنترل دسترسی پیکربندی دور کند.

بنابراین خدمات میزبانی وب، سازمان‌هایی که سرورهای خود و مدیران وب را مدیریت میکنند، به شدت توصیه میشوند که آپاچی HTTP خود را به آخرین نسخه در اسرع وقت ارتقا دهند.

گردآورنده: امیرحسین ضرغامی

وصله‌های امنیتی برای رفع آسیب پذیری‌های متعدد در NVIDIA

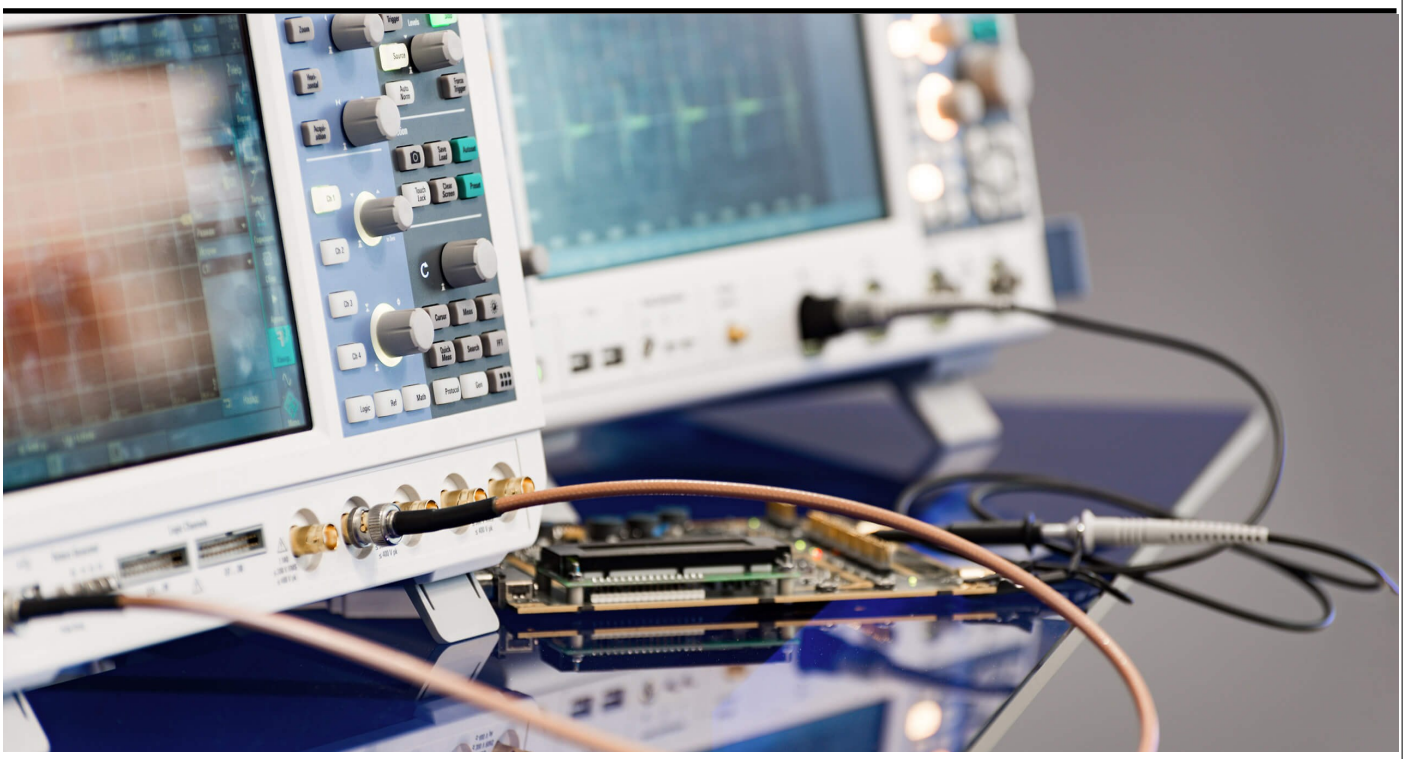
شرکت بزرگ تولید کننده‌ی کارت‌های گرافیک بسیار محبوب NVIDIA چند مدتی است که درگیر آسیب پذیری‌های شده است که بسیار بر نام و اعتبار این شرکت تاثیر گذاشته است.

این هفته NVIDIA وصله‌های امنیتی را برای رفع آسیب پذیری‌های متعدد در Linux Driver Package L4T منتشر کرد، از جمله چند نقص بحرانی با ارزیابی درجه بالا. مهمترین اشکالات CVE-2018-6269، یک آسیب پذیری است که درکرنل Tegra ساکن است. (VSS 8.8) این کنترل دستیابی به ورودی / خروجی (IOCTL) را برای درخواست حالت کاربر

تحت تاثیر قرار می دهد و می تواند منجر به افشای اطلاعات، انکار سرویس (DoS)، تشدید امتیازات یا اجرای کد شود.دومین و جدی ترین آسیب پذیری آن، بر اساس نمره CVSS آن ۸.۴، CVE-2017-6278 می باشد.که درایور های ولتاژفرکانس های پویا در هسته تگرا (DVFS) سبب این مشکل هستند، این آسیب پذیری امکان می دهد خواندن یا نوشتن یک بافر با استفاده از شاخص یا اشاره گر که به محل حافظه پس از پایان بافر اشاره می کند، که ممکن است منجر به انکار سرویس یا تشدید امتیازات اجرایی شود. سومین خطای شدید (CVE-2018-6267)، نمره CVSS 8.4 در درایور Tegra OpenMax (libnvomx) یافت شده و شامل یک چک لیست متادیتا کاربر می شود که می تواند ابردادهای نامعتبر را به عنوان معتبر به تصویب برساند و در نتیجه یک وضعیت DoS یا تشدید امتیازات اجرایی در نظر بگیرداکثر این آسیب پذیری ها نیاز به دسترسی محلی به سیستم هدف دارد.

گردآورنده: امیرحسین ضرغامی

روش جدید محققان برای کشف بدافزارهای پنهان در سخت افزارها



نرم افزارها همیشه قادر به کشف بدافزارهای موجود در فریمورهای سخت افزارها نیستند. تشخیص هک‌های سخت افزاری به شدت دشوار بوده اما پیشرفتی بزرگ در جلوگیری از این حملات به تازگی صورت گرفته است.

پنهان کردن نرم افزارهای مخرب داخل درایوهای سخت افزاری، مادربرد، کارت گرافیک و دیگر اجزای رایج در سطح سیستم عامل، تشخیص هرگونه فعالیت خلافکارانه را تفریبا غیر ممکن می‌کند.

محققان دانشگاه ایالتی کارولینای شمالی و دانشگاه تگزاس، روش‌های قابل اعتمادی برای شناسایی چنین نفوذاتی را توسعه داده‌اند. با مشخص کردن توان مصرفی سیستم و هر یک از اجزای آن، نوع بدافزار موجود می‌تواند تعیین گردد. این تحقیقات توسط موسسه Lockheed Martin و بنیاد ملی علوم حمایت شده است.

رایانه‌های رومیزی برنامه اصلی این نوآوری نیستند. دستگاه‌های مربوط به اینترنت اشیا و سیستم‌های پیاده سازی شده در صنایع موارد مهم استفاده این نوآوری هستند که باید به آنان نگاهی انداخت. بسیاری از این دستگاه‌ها دارای سیستم عامل نیستند و تنها کد دستگاه را اجرا می‌کنند که در بخش کوچکی از حافظه غیر قابل ذخیره نگهداری می‌شود. نرم افزار آنتی ویروس در اکثر سیستم‌های Embedded در دنیای واقعی عملی نیست.

مانیتور کردن قدرت مصرفی وسایل به تنهایی یک ایده‌ی جدید نمی‌باشد اما ایده‌ی ایجاد یک وسیله‌ی با قابلیت نصب آسان برروی وسایل مختلف بسیار جذاب است.

تنها نکته اینجا این است که نرم افزارهای مخرب بسیار دقیق می‌توانند تلاش کنند که مصرف برق طبیعی را تکرار کنند. در این موارد، زمانی وجود دارد که ابزار ارائه شده قادر به تشخیص حضور نرم افزارهای مخرب نیست. با این حال، در تحقیقات، سرقت اطلاعات توسط نرم افزارهای مخرب به میزان ۸۶ تا ۹۷ درصد کاهش پیدا کرد.

گردآورنده: محمد مرتضوی

تبدیل شرکت‌های آسیایی را به یک ماینر Monero

تیم امنیت نرم افزار شرکت Symantec روز چهرشنبه خبری را در وبلگ خود انتشار داد که براساس آن، ۸۰ درصد از قربانیان این بدافزار در چین وبا ملیت کره جنوبی، ژاپن و ویتنام هستند.

این شرکت ادعا کرده است که کد مخرب Beapy بر خلاف اکثر بدافزارهایی که بر مبنای مرورر هستند براساس فایل می‌باشد. این بدافزار با ارسال فایل آلوده‌ی اکسل به قربانیان از طریق ایمیل و با دانلود درب پشتی DoublePulsarفعالیت خود را آغاز می‌کند.

بدافزار DoublePulsar (که توسط NSA توسعه داده شده است) همچنین در حملات مربوط به WannaCry در سال ۲۰۱۷ نیز مورد استفاده قرار گرفت.

به محض اینکه DoublePulsar برروی سیستم قربانی نصب گردد اقدام به دانلود Miner خواهد کرد. در همین لحظه این بدافزار از یکی دیگر از ابزارهای لو رفته‌ی NSA به نام EternalBlue استفاده می‌کند تا در سراسر شبکه و برروی کامپیوترهای بدون وصله امنیتی برای سرقت اطلاعات گسترش یابد.

براساس اعلام Symantec، بدافزارهایی که سارق ارز رمز هستند می‌توانند تاثیرات بسیار زیادی را برروی شرکت‌ها داشته باشند همانند افت سرعت و کارایی، افت بهره وری و افزایش هزینه‌ها. اگر چه فعالیت رمزنگاری در سال گذشته در حدود ۵۲ درصد کاهش یافته است، اما هنوز هم هکرهایی در این میان هستند که به طور عمده به این نو کسب و کارها علاقه دارند.

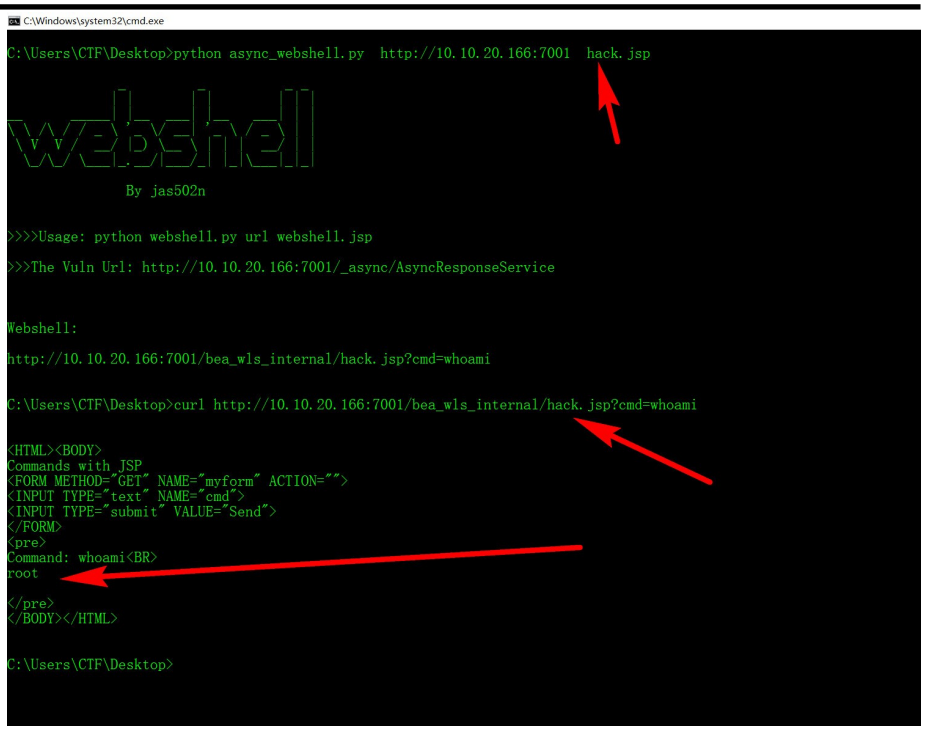
شرکت Symantec اعلام نمود که اولین ردگیری از این بدافزار در ماه ژانویه اتفاق افتاده است اما فعالیت این بدافزار در ماه مارچ با افزایش چشمگیری مواجه شده است.

ویژگی‌های بالای امنیتی و حریم موجود در این ارز رمز باعث شده است تا در میان هکرهای تولید کننده‌ی بدافزار، محبوبیت بالایی را کسب کند. تحقیقات دانشگاهی اخیر نشان می‌دهد که در حدود ۵ درصد از استخراج ارز رمز Monero مربوط به مجرمان سایبری می‌باشد.

در ابتدای امسال محققان امنیتی در شرکت Palo Alto بدافزار جدیدی را کشف کردند که توانایی در اختیار گرفتن کنترل Admin سیستم برای حذف محصولات امنیتی و سپس تزریق کدهای مخرب استخراج کننده-ی Monero را دارد. این تیم همچنین موفق به کشف انواع متنوعی از بدافزارهای سارق Cookie های مرورگرها و سایر اطلاعات برروی کامپیوترهای Mac شدند.

گردآورنده: محمد مرتضوی

نقص بحرانی روز صفر در سرور اوراکل WebLogic



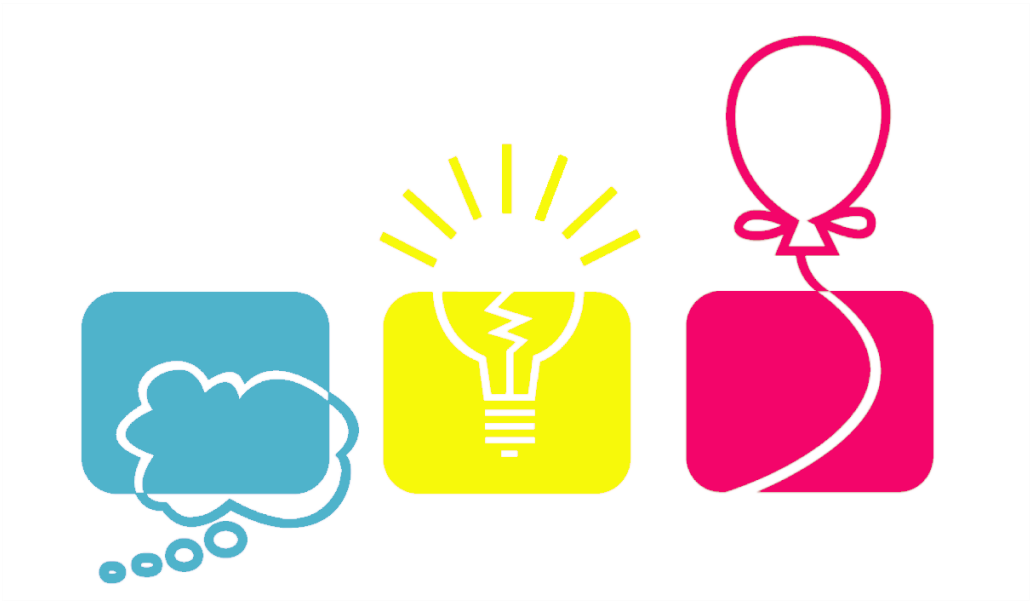
محققان امنیتی یک نقص "بسیار بحرانی" روز صفر را در سرور اوراکل WebLogic کشف کرده اند که این نقص بر تمامی نسخه های WebLogic تاثیر می گذارد. آسیب پذیری اجازه می دهد تا هکرها بتوانند کد های دلخواه را از راه دور اجرا کنند. این نقص، به نام "CNVD-C-2019-48814"، تاثیر گزار بر روی همه نسخه های WebLogic است، از جمله آخرین به روز رسانی آن می باشد: wls9_async_response.warو wls-wsat.war

WebLogic اوراکل یک ابزار مبتنی بر جاوا است که کاربران را قادر می سازد تا برنامه های سازمانی چند لایه را از طریق ابر توسعه دهند. مجرمان سایبری قادر به بهره برداری از این آسیب پذیری بدون مجوز و با جمع آوری یک درخواست HTTP مخرب هستند. پلت فرم اشتراک گذاری آسیب پذیری اطلاعات ملی چین (CNVD) توضیح داد که چگونه این نقص کار می کند: "از آنجا که بسته WAR دارای نقصی در نادیده گرفتن اطلاعات ورودی است، مهاجم می تواند مجوز سرور مقصد را با ارسال یک درخواست HTTP مخرب به دقت ساخته شده است را بدست آورد. و فرمان را از راه دور و بدون مجوز اجرا می کند."

اگر چه مشخص نیست که چگونه بسیاری از کاربران ممکن است تحت تاثیر آسیب پذیری قرار بگیرند ولی ر حال حاضر بیش از ۱۰۱,۰۴۰ سرور WebLogic در اینترنت وجود دار که ۳۶,۱۷۳ آن در چین و آمریکا می باشد. به طور معمول اوراکل به روز رسانی های امنیتی خود را هر سه منتشر می کند و شاید زمان کمی داشته باشد تا به حل این مشکل به پردازد. علیرغم هشدار ها به اوراکل ممکن است پیش از آنکه شرکت به این مسئله پاسخ دهد، خسارات زیادی بر کاربران وارد شود و اما راه کارهای فعلی برای رفع این مشکل تا آمدن به روز رسانی جدید پاک کردن wls-wsat است.

گردآورنده: امیرحسین ضرغامی

KHARAZMI CERT COORDINATOR CENTER



مرکز آپا دانشگاه خوارزمی

رییس مرکز:

دکتر امید مهدی عبادتی

اعضای هیات علمی:

دکتر احسان ملکیان

دکتر امید مهدی عبادتی

کارشناسان مرکز:

محمدحسین خدامی

سمیه نیا خلیلی

محمد مرتضوی

امین زمانی

حسین علیمرادی

شیوا بهادری

امیرحسین ضرغامی

محسن یزدی‌نژاد

فاطمه الهی

نشانی:

کرج - دانشگاه خوارزمی - کتابخانه‌ی مرکزی - طبقه‌ی همکف - مرکز آپا

تلفن:

۰۲۶۳۴۵۷۵۰۱۲

۰۲۶۳۴۵۷۵۰۱۸

۰۲۶۳۴۵۷۹۶۰۰ (داخلی ۲۶۲۲)

پست الکترونیک:

cert@khu.ac.ir

وب سایت:

https://cert.khu.ac.ir/

کانال مرکز آپا خوارزمی:

@khu_cert

دانلود رایگان:

دانلود رایگان مجموعه کامل خبرنامه‌ها از طریق اسکن کد زیر در دسترس است.