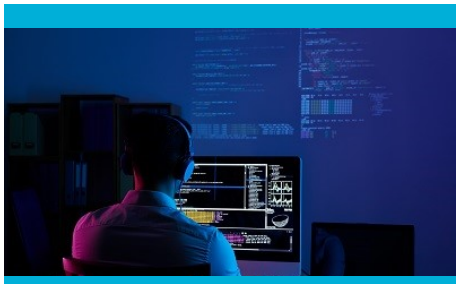
شماره سی و چهارم - شهریور ۱۳۹۹

خبرنامه "آپا" دانشگاه خوارزمی

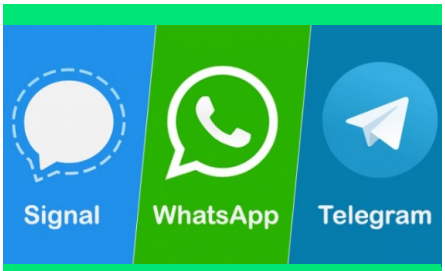
KHARAZMI CERT
COORDINATION CENTER
مرکز تخصصی آپا خوارزمی

در این شماره خواهید خواند:



معرفی ۵ زبان برنامه نویسی برای دوستداران امنیت

اگر شما مدیر امنیت شرکتی هستید که قصد ارتقاع مهارت‌های خود را دارید و یا به تازگی قدم در راه امنیت گذاشته‌اید بهتر است تا در خصوص مزایای یادگیری یک زبان برنامه نویسی در حوزه‌ی امنیت شبکه و اپلیکیشن به تحقیق بپردازید. صفحه ۲



جاسوسی از طریق دوربین موبایل‌های اندرویدی

محققان می‌گویند پیام رسان‌های مشهور تلفن همراه مانند WhatsApp از طریق سرویس‌های discovery، اطلاعاتی را در اختیار شما قرار می‌دهند که به کاربران امکان می‌دهد مخاطبین خود را بر اساس شماره تلفن از دفترچه آدرس خود پیدا کنند. - صفحه ۳

بزرگ‌ترین هک خودکار مجنتو در پنج سال گذشته!

از زمان اعلام پایان چرخه محصول نسخه یک سیستم مدیریت محتوای مجنتو در ژانویه سال ۲۰۲۰، فروشگاه‌های تجارت الکترونیکی با نسخه قدیمی مجنتو (نسخه ۱) با خطر حملات سایبری روبه‌رو شده‌اند. در همین راستا، در ماه آپریل، شرکت ویزا از تجار آنلاین خواسته بود که زیرساخت‌های خود را به نسخه جدید (Magento 2.x) آپدیت کنند. - صفحه ۴

سرقت اطلاعات شخصی Discord توسط بدافزار جدید!

مراقب باشید که یک بدافزار جدید منتشر شده. این بدافزار که با نام 'Spidey Bot' شناخته می‌شود بسیار خطرناک بوده چرا که می‌تواند تمام اطلاعات شخصی شما مثل رمزهای‌عبور، ایمیل‌ها، آدرس‌های آی‌پی، مخاطبین و نام‌های کاربری Discord را به سرقت ببرد.این بدافزار ویندوز این کار را از طریق قرار دادن خود در کدهای اپلیکیشن Discord انجام می‌دهد. - صفحه ۵

افشای اطلاعات جستجوی کاربران توسط سرورهای ناامن بینگ!

یکی از سرورهای مربوط به مایکروسافت اطلاعات مهمی را از قبیل نتایج جستجوی کاربران، جزییات مربوط به دیوایسی‌ها و اطلاعات GPS و منطقه‌ای آنان را افشا نموده است. این دیتابیس که مخصوص نگهداری لاگ‌ها می‌باشد خوشبختانه اطلاعات حساس همانند نام، نام کاربری و آدرس کاربران را در خود ذخیره نمی‌کند. - صفحه ۶

نسخه جدید فایرفاکس و رفع آسیب پذیری اجرای کد از دور

موزیلا چندین آسیب پذیری با درجه اهمیت بالا را در فایرفاکس ۸۱ و فایرفاکس ESR ۷۸.۳ که امکان اجرای کد از راه دور را مهاجمان می‌دادند رفع کرد. - صفحه ۷

معرفی ۵ زبان برنامه نویسی برای دوستداران امنیت

اگر شما مدیر امنیت شرکتی هستید که قصد ارتقاع مهارت‌های خود را دارید و یا به تازگی قدم در راه امنیت گذاشته‌اید بهتر است تا در خصوص مزایای یادگیری یک زبان برنامه نویسی در حوزه‌ی امنیت شبکه و اپلیکیشن به تحقیق بپردازید.

داشتن دانش پایه از زبان‌های برنامه نویسی می‌تواند به فعالین این حوزه در ایجاد ابزار، خودکار سازی فرآیندها و نوشتن Shell Script کمک شایانی کند. در این مقاله قصد داریم تا با معرفی ۵ زبان برنامه نویسی و مزایای هر یک از آنان به شما نشان دهیم تا چرا برای تبدیل شدن به یک مدیر امنیت نیاز است تا برنامه نویسی را یاد بگیرید.

- **زبان برنامه نویسی C**

یک زبان برنامه نویسی سطح پایین می‌باشد که در ۵ دهه‌ی اخیر به وفور مورد استفاده قرار گرفته است و قابلیت Cross-Platform شدن در آن نیز تعبیه گردیده است. با پیاده سازی صحیح ساختار، به راحتی و با چندین تغییر کوچک می‌توانید برنامه‌های تولید شده‌ی خود را در این زبان، در تمامی سیستم عامل‌ها اجرا نمایید.

به دلیل سطح پایین بودن این زبان برنامه نویسی، برنامه نویس تعامل بسیار بالایی با سخت افزار دارد. لذا محققان امنیت برای بررسی تهدیدات در سطح سخت افزار نیز می‌توانند از این زبان برنامه نویسی استفاده کنند.

- **زبان برنامه نویسی Python**

یکی از پیشرفته‌ترین زبان‌های برنامه نویسی سطح بالا با قابلیت Cross-Platform می‌باشد. این زبان برنامه نویسی دارای انجمن‌ها و حامیان بسیاری است که روز به روز در حال گسترش می‌باشد. زبان‌های نوشته شده با این زبان برنامه نویسی با استفاده از ابزارهای موجود، قابلیت اجرا برروی تمامی سیستم عامل‌ها را دارا می‌باشند. این زبان برنامه نویسی در حوزه‌ی امنیت بیشتر توسط Red Team (تیم قرمز) و برای شبیه سازی حملات یا تست نفوذ مورد استفاده قرار می‌گیرد.

- **زبان برنامه نویسی JavaScript**

در حالی که JS یک زبان اسکریپت نویسی است اما به وفور مورد استفاده قرار می‌گیرد. به طور میانگین بیش از ۹۷٪ از وب سایت‌ها از این زبان استفاده می‌کنند.

محققان امنیتی از این زبان برای بررسی حملات سمت مشتری یا Client استفاده می‌کنند. حملاتی همچون XSS، CSRF، Request Tampering با استفاده از این زبان قابل پیاده سازی است.

- **زبان برنامه نویسی PHP**

این زبان برنامه نویسی که بیشتر در حوزه‌ی وب کاربرد دارد یکی از زبان‌های پرکاربرد در امنیت می‌باشد. CMS های بسیاری با این زبان توسعه داده شده‌اند که این امر باعث می‌شود تا محققان امنیتی شروع به توسعه‌ی Exploit برای نفوذ به این وب سایت‌ها با این زبان کنند.

با استفاده از این زبان برنامه نویسی Backdoor های فراوانی توسعه داده شده است و نفوذگران با استفاده از آنان می‌توانند کنترل سامانه‌های قربانی را به دست گیرند.

- **زبان SQL**

زبان کوئری نویسی درواقع روشی برای فراخوانی داده‌های مختلف از پایگاه‌های داده می‌باشد. اکثریت بالایی از وب سایت‌ها برای ذخیره و نمایش داده‌های خود از پایگاه داده استفاده می‌کنند که همین امر یادگیری این زبان را برای محققان امنیتی ضرروی می‌کند. با دانستن این زبان می‌توان حملاتی همچون SQL injection، Data Leakage و... طراحی و پیاده سازی نمود.

گردآورنده: محمد مرتضوی

WhatsApp و Telegram آن‌قدرها هم ایمن نمی‌باشند!

محققان می‌گویند پیام رسان‌های مشهور تلفن همراه مانند WhatsApp از طریق سرویس‌های discovery، اطلاعاتی را در اختیار شما قرار می‌دهند که به کاربران امکان می‌دهد مخاطبین خود را بر اساس شماره تلفن از دفترچه آدرس خود پیدا کنند. هنگام نصب یک پیام‌رسان تلفن همراه مانند WhatsApp، کاربران جدید می‌توانند بلافاصله پیام‌های تماس موجود را بر اساس شماره تلفن‌های ذخیره شده در دستگاه خود شروع کنند. برای این اتفاق، کاربران باید در فرآیندی به نام کشف مخاطب تلفن همراه، به برنامه اجازه دسترسی و بارگذاری مرتب دفترچه آدرس خود را در سرورهای شرکت بدهند.

مطالعه‌ای از دانشگاه فنی دارمشتات و دانشگاه وورتسبورگ آلمان نشان می‌دهد که در حال حاضر سرویس‌های کشف تماس موجود، حریم خصوصی میلیاردها کاربر را به شدت تهدید می‌کنند. محققان با استفاده از منابع بسیار اندک توانستند حملات عملیاتی crawling به پیام‌رسان‌های محبوب WhatsApp، Signal و Telegram انجام دهند. نتایج آزمایشات نشان می‌دهد که کاربران مخرب یا هکرها می‌توانند با پرس‌وجو از خدمات کشف مخاطب برای شماره تلفن‌های تصادفی، اطلاعات حساس را در مقیاس وسیع و بدون محدودیت قابل توجه جمع آوری کنند.

برای این مطالعه، محققان ۱۰ درصد از کل شماره تلفن‌های تلفن همراه ایالات متحده را برای WhatsApp و ۱۰۰ درصد را برای Signalجستجو کردند.

بدین ترتیب، آن‌ها قادر به جمع آوری داده‌های شخصی (متا) معمولاً ذخیره شده در پروفایل کاربری پیام‌رسان‌ها، از جمله تصاویر پروفایل، نام‌های مستعار، متن وضعیت و آخرین بار آنلاین بودند.

داده‌های تجزیه و تحلیل شده هم‌چنین آمار جالبی را در مورد رفتار کاربر نشان می‌دهد. به عنوان مثال، تعداد بسیار کمی از کاربران تنظیمات حریم خصوصی پیش‌فرض را تغییر می‌دهند، که برای اکثر پیام‌رسان‌ها به هیچ وجه حریم خصوصی محسوب نمی‌شود.

محققان دریافتند که حدود ۵۰ درصد از کاربران WhatsApp در ایالات متحده دارای یک عکس پروفایل عمومی و ۹۰ درصد دارای یک متن عمومی "درباره" هستند. جالب توجه است که ۴۰ درصد از کاربران Signal، که به طور کلی می‌توان گفت بیشتر به حریم خصوصی توجه می‌کنند، از WhatsApp نیز استفاده می‌کنند و سایر کاربران سیگنال دارای یک عکس پروفایل عمومی در WhatsApp هستند. ردیابی چنین داده‌هایی با گذشت زمان، مهاجمان را قادر می‌سازد مدل‌های دقیق رفتاری را ایجاد کنند. هنگامی که داده‌ها در شبکه‌های اجتماعی و منابع داده عمومی همسان می‌شوند ، اشخاص ثالث هم‌چنین می‌توانند پروفایل‌های مفصلی به عنوان مثال برای کلاه‌برداری ایجاد کنند.

برای Telegram، محققان دریافتند که سرویس کشف مخاطب آن اطلاعات حساسی را حتی در مورد دارندگان شماره تلفن‌هایی که در این سرویس ثبت نشده‌اند، نشان می‌دهد. محققان می‌گویند که کدامین اطلاعات در هنگام کشف مخاطب فاش می‌شود و می‌تواند از طریق حملات crawling جمع آوری شود که به ارائه دهنده خدمات و تنظیمات حریم خصوصی کاربر بستگی دارد.

از آن‌جا که هیچ محدودیتی قابل توجه برای ثبت نام در خدمات پیام‌رسانی وجود ندارد، هر شخص ثالثی می‌تواند تعداد زیادی حساب ایجاد کند تا بتواند با درخواست داده برای شماره تلفن‌های تصادفی، پایگاه داده کاربر پیام‌رسان را جستجو کند.

محققان می‌گویند که ما اکیداً به همه کاربران برنامه‌های پیام‌رسان توصیه می‌کنیم که از تنظیمات حریم خصوصی خود بازدید کنند. این مطالعه قرار است در فوریه ۲۰۲۱ در بیست و هشتمین سالانه همایش امنیت شبکه و سیستم توزیع شده (NDSS) که یک کنفرانس برتر برای امنیت فناوری اطلاعات است، منتشر شود.

گردآورنده: امین زمانی

بزرگ‌ترین هک خودکار مجنتو در پنج سال گذشته!

از زمان اعلام پایان چرخه محصول نسخه یک سیستم مدیریت محتوای مجنتو در ژانویه سال ۲۰۲۰، فروشگاه‌های تجارت الکترونیکی با نسخه قدیمی مجنتو (نسخه ۱) با خطر حملات سایبری روبه‌رو شده‌اند. در همین راستا، در ماه آپریل، شرکت ویزا از تجار آنلاین خواسته بود که زیرساخت‌های خود را به نسخه جدید (Magento 2.x) آپدیت کنند. اخیراً یک کارزار (Magecart)، هزاران فروشگاه تجارت الکترونیک آسیب‌پذیر را در سطح جهان با یک اسکیمر مورد هدف قرار داده است.

به گزارش Sanguine Security (Sansec)، بیش از ۲۰۰۰ سایت مجنتو نسخه ۱، برای سرقت جزئیات کارت اعتباری با یک اسکریپت اسکیمینگ خودکار مورد حمله قرار گرفتند. در ۱۱ سپتامبر، ده فروشگاه به یک اسکریپت منحصر به فرد کارت اعتباری آلوده شدند که تعداد آن در روز بعد با هک شدن ۱۰۵۸ سایت، ۶۰۳ مورد دیگر در ۱۳ سپتامبر و ۲۳۳ مورد دیگر در ۱۴ سپتامبر با یک الگوی حمله کلاسیک، افزایش یافت.

مهاجمان از ویژگی Magento Connect برای بارگیری و نصب چندین فایل مخرب از جمله درب پشتی موسوم به mysql.php استفاده کردند و هنگام افزودن کد به prototype.jsسایت‌های مجنتو نسخه ۱ و jquery.js سایت‌های مجنتو نسخه ۲، این فایل‌ها را به طور خودکار حذف کردند.

این کارزار با شناسایی آسیب‌پذیری روز صفر که توسط یک مهاجم به نام z3r0day در ماه آگوست در فروم‌های هکری فروخته می‌شد، آغاز شد. در چند ماه گذشته تعداد سایت‌های تجارت الکترونیکی که توسط Magecart و گروه‌های مرتبط مورد هدف قرار گرفته‌اند، افزایش یافته است. مهاجمان Magecartدر هنگام استفاده از سرویس پیام‌رسانی رمزگذاری‌شده تلگرام برای انتقال غیرمجاز اطلاعات، یافت شدند.

در ماه جولای، مهاجمان با استفاده از حمله Magecart فروشگاه‌های آنلاین خرده‌فروشان و سازمان‌های بزرگ ایالات متحده مانند Technokain Solutions ، Consumer Electronics Show، Consumer Technology and Association، Claire را هدف قرار دادند. در ماه ژوئن، گروه Magecart وب‌سایت‌های هشت شهر ایالات متحده را در سه ایالت با اسکیمرهای Magecart که سرقت کارت پرداخت انجام می‌دادند، هدف قرار داده بود.

مقیاس عظیم آخرین حوادث ماه سپتامبر ، افزایش پیچیدگی و سودآوری استفاده از وب اسکیمینگ را نشان می‌دهد. حملات MageCart به یک مشکل بزرگ برای تمام توسعه دهندگان و کاربران مجنتو تبدیل شده است. برای امنیت بهتر، توصیه می‌شود همه زیرساخت‌های خود را در اسرع وقت ارتقا دهید.

گردآورنده: امین زمانی

سرقت اطلاعات شخصی Discord توسط بدافزار جدید!

مراقب باشید که یک بدافزار جدید منتشر شده. این بدافزار که با نام 'Spidey Bot' شناخته می‌شود بسیار خطرناک بوده چرا که می‌تواند تمام اطلاعات شخصی شما مثل رمزهای‌عبور، ایمیل‌ها، آدرس‌های آی‌پی، مخاطبین و نام‌های کاربری Discord را به سرقت ببرد.این بدافزار ویندوز این کار را از طریق قرار دادن خود در کدهای اپلیکیشن Discord انجام می‌دهد.

این بدافزار همچنین قادر به ایجاد یک بک‌دور به دستگاه شما از طریق کپی کردن ۵۰ کلمه اول تایپ شده بوسیله کیبورد شما که ممکن است اطلاعات حساسی مثل رمزهای عبور وارد شده باشد است. این عمل برای ارسال بدافزارهای بیشتر به دستگاه انجام می‌شود.

Discord یک اپلیکیشن است که بطور خاص برای جامعه بازی‌های رایانه‌ای ساخته شده. این اپلیکیشن همچنین یک پلتفرم دیجیتال است که گیمرهای مختلف از نقاط مختلف جهان با هم ارتباط برقرار کرده و یک اجتماع خود را تشکیل می‌دهند.

اخیرا Discord به یک پلتفرم ایده‌آل برای کاربرانی که بخاطر نظرات توهین‌آمیز از توییتر یا Reddit بیرون انداخته شده‌اند تبدیل شده، لذا در اینجا آزاد به انتشار نظرات خود خواهند بود. متاسفانه فهم اینکه آیا فایل Discord شما آلوده است یا خیر ممکن نیست و حتی اگر متوجه این امر شوید قادر به کاری نخواهید بود. بهترین کاری که از دست شما بر می‌آید پاک کردن نرم افزار و نصب دوباره آن برای اطمینان از امن بودن است.بنابراین داشتن بهترین آنتی‌ویروس تنها راه حل از جلوگیری از خطر بدافزارها می‌باشد حتی اگر کمپانی نرم‌افزار Discord در حل مشکلات کاربران توانا نباشد.

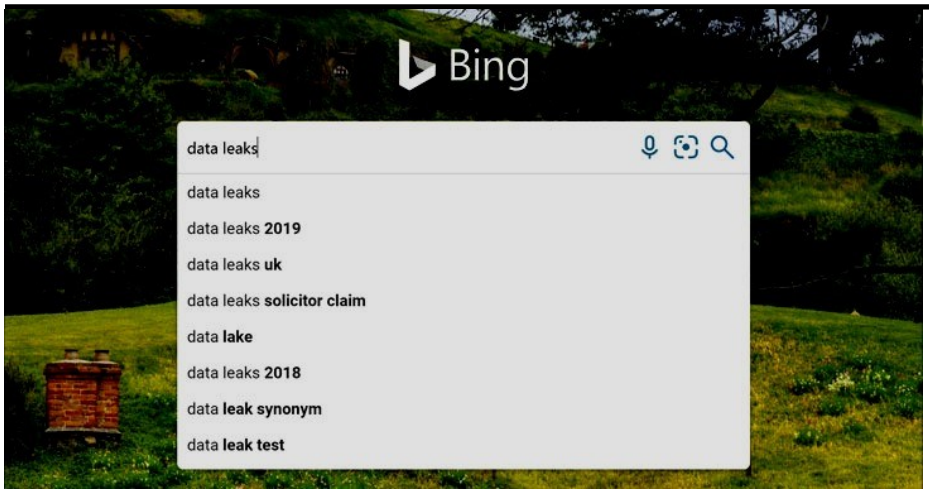
Discord در پاسخ به شکایات توییت کرد:

"متاسفانه از دست Discord کاری برای پیش‌بینی خطر در نمی‌آید. اما کاربران باید در هنگام کلیک کردن روی لینک‌های ناشناس مراقب بوده و نسبت به دانلود نرم‌افزارهای نا آشنا حساس باشند.انجام این کار ممکن است باعث دریافت بدافزار شود. نصب یک برنامه غیرقابل اعتماد می‌تواند باعث تغییر Discord روی کامپیوتر شما شود".

تنها راهکار دیگر برای خطر این بدافزار درخواست از کاربران برای استفاده از اپلیکیشن Discord روی تلفن‌همراه و کنسول بجای کامپیوتر است.

گردآورنده: حسین علیمرادی

افشای اطلاعات جستجوی کاربران توسط سرورهای ناامن بینگ!



یکی از سرورهای مربوط به مایکروسافت اطلاعات مهمی را از قبیل نتایج جستجوی کاربران، جزییات مربوط به دیوایسی‌ها و اطلاعات GPS و منطقه‌ای آنان را افشا نموده است.

این دیتابیس که مخصوص نگهداری لاگ‌ها می‌باشد خوشبختانه اطلاعات حساس همانند نام، نام کاربری و آدرس کاربران را در خود ذخیره نمی‌کند.

اطلاعات مذکور در تاریخ ۱۲ سپتامبر نشر پیدا کرده است که حجم آن چیزی در حدود ۶.۵ ترابایت از دسترسی کاربران به موتور جستجوی بیگ است که هیچ پسوردی برروی آن تنظیم نگردیده است. این اطلاعات می-تواند توسط گروه‌های مختلف و مجرمان سایبری برای انجام انواع حملات فیشینگ مورد استفاده قرار گیرد.

براساس گزارش WizCase این اطلاعات تا ۱۰ سپتامبر توسط پسورد محافظت می‌شدند اما بعد از آن این پسورد به صورت ناخواسته حذف گردیده است.

بعد از گزارش این نقص به مرکز پاسخ به رخ دادهای امنیتی مایکروسافت، در تاریخ ۱۶ سپتامبر این مشکل مرتفع گردید.

وجود نقص در تنظیمات سرویس دهنده یا همان misconfiguration در سال‌های اخیر باعث نشت اطلاعات حساس بسیاری در فضای اینترنت گردیده است.

براساس گزارش WizCase اطلاعات نشت پیدا کرده مربوط به کاربران از ۷۰ کشور مختلف می‌باشد.

علاوه بر اطلاعات مربوط به جستجوها و منطقه‌ی مکانی افراد، زمان دقیق جستجو و صفحات مشاهده توسط کاربران، سه شناسه‌ی یکتا همانند ADID، DeviceID و Devicehash نیز نشر پیدا کرده است.

همچنین سرور مذکور پیش تر نیز توسط meow attack دوبار مورد حمله قرار گرفته بود. این حمله، یک حمله‌ی خودکار بود که دیتای بیش از ۱۴۰۰۰ دیتابیس ناایمن را پاک کرده بود.

براساس اطلاعات درز پیدا کرده محققان امنیتی ادعا دارند که هکرها حالا با دانستن عباراتی که مردم هر کشور بیشتر مورد جستجو قرار داده‌اند می‌توانند حملات خود را با موفقیت بالاتری برای مردمان کشورهای مختلف بهینه کنند و آنان را هدف blackmail قرار دهند.

گردآورنده: محمد مرتضوی

نسخه جدید فایرفاکس و رفع آسیب پذیری اجرای کد از دور

موزیلا چندین آسیب پذیری با درجه اهمیت بالا را در فایرفاکس ۸۱ و فایرفاکس ESR ۷۸.۳ که امکان اجرای کد از راه دور را مهاجمان می‌دادند رفع کرد.

دو باگ با شناسه‌های CVE-2020-15674 و CVE-2020-15673 باعث ایجاد خطا در سیستم محافظتی حافظه‌ی مرورگر می‌شوند که در نهایت باعث ایجادی مشکلات همچون Overflow می‌گردند.

آسیب پذیری به شناسه‌ی CVE-2020-15674 تنها در فایرفاکس نسخه‌ی ۸۰ گزارش شده بود ولی آسیب پذیری با شناسه‌ی CVE-2020-15673 هم در فایرفاکس نسخه‌ی ۸۰ و هم در فایرفاکس ESR نسخه‌ی ۷۸.۲ گزارش شده بودند.

بر اساس اعلام مزیلا، برخی از این آسیب پذیری‌ها باعث ایجاد خطا و نقص در حافظه می‌شدند و ما فرض را بر این گذاشتیم که با تلاش کافی می‌توان از این آسیب پذیری‌ها در جهت اجرای کد دلخواه از راه دور استفاده کرد.

براساس گزارش موزیلا این دو آسیب پذیری دارای درجه‌ی اهمیت بالا (High) هستند که به می‌توانند برای اعمالی چون جمع آوری اطلاعات از سایت‌ها یا تزریق داده و کد در وب سایت‌ها مورد استفاده قرار گیرند.

در نسخه‌ی ۸۱ فایرفاکس همچنین آسیب پذیری با درجه اهمیت بالای دیگر که مربوط به کتابخانه‌ی گرافیکی وب می‌باشد نیز رفع گردیده است.

این آسیب پذیری در بخش مذکور مربوط به نوع use-after-free است که یکی از آسیب پذیری‌های مربوط به استفاده‌ی نادرست از حافظه‌ی پویا می‌باشد. اگر پس از آزاد کردن مکان حافظه‌ای، برنامه‌ای نشانگر مربوطه به آن خانه از حافظه را پاک نکند، مهاجم می‌تواند با استفاده از خطا برنامه را هک کند. سوء استفاده از آسیب پذیری یاد شده دارای پیچیدگی بالایی می‌باشد اما استفاده از آن غیر ممکن نمی‌باشد.

در ضمن آسیب پذیری‌های یاد شده، چندین آسیب پذیری دیگر نیز توسط موزیلا در نسخه‌ی جدید فایرفاکس رفع گردید که عبارتند از:

- CVE-2020-15677
- CVE-2020-15676
- CVE-2020-15678

نسخه‌ی جدید فایرفاکس هم اکنون در دسترس قرار گرفته است و کاربران می‌توانند مرورگرهای خود را به این نسخه به روز رسانی کنند.

برای دریافت این نسخه می‌توان به وب سایت رسمی موزیلا به آدرس زیر مراجعه کرد.

https://www.mozilla.org/

گردآورنده: محمد مرتضوی

KHARAZMI CERT COORDINATION CENTER

مرکز آپا دانشگاه خوارزمی

رئیس مرکز:

دکتر امید مهدی عبادتی

اعضای هیات علمی:

جناب آقای دکتر عبادتی

سرکار خانم دکتر یعقوبی

کارشناسان مرکز:

محمدحسین خدامی

سمیه نیا خلیلی

محمد مرتضوی

امین زمانی

حسین علیمرادی

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.

معاونت پژوهش و فناوری