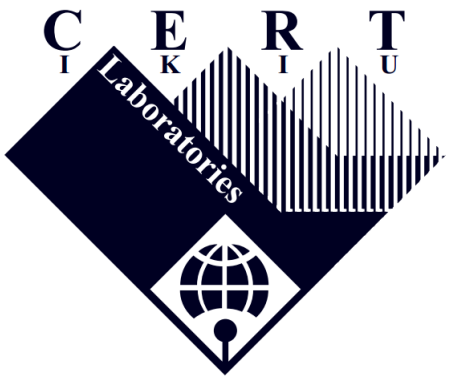

آزمایشگاه تخصصی آپا، قزوین

دانشگاه بین المللی امام خمینی (ره)

هفته نامه تحلیلی رویدادهای امنیتی

شنبه ششم مهر ماه ۱۳۹۸

نسخه ۱,۰,۰

بنام خداوند بخشنده و مهربان

یادداشت سردبیر

استخراج‌گر غیرمجاز ارز دیجیتال[1] نوع جدیدی از بدافزار[2]ها بوده که با سوءاستفاده از قدرت پردازشی سیستم قربانی به کسب درآمد برای مهاجم می‌پردازد. در بسیاری از موارد این نوع بدافزارها با بررسی افزایش بهره‌گیری از منابع پردازشی (نظیر سی.پی.یو [3]و جی.پی.یو[4]) قابل کشف و مقابله است. در هفته گذشته نوع پیشرفته‌ای از بدافزارهای مذکور به دنیای امنیت اطلاعات معرفی شده و توجه بسیاری از محققان سایبری را به خود جلب کرد. این بدافزار اِسکیدمَپ[5] نام داشته که مهاجمان به کمک روت.کیت[6]ها باعث پیچیدگی بسیار بالای تشخیص آن شده‌اند. روت.کیت‌ها نوع دیگری از بدافزارها بوده که جایگزین فایل‌های سیستم‌عامل شده و فعالیت غیرمجاز خود را قانونی نشان می‌دهند. ترکیب استخراج ارز دیجیتال و روت.کیت در بدافزار اِسکیدمَپ باعث سختی شناسایی فعالیت مخربانه شده چرا که این امر به کمک سیستم‌عامل قانونی و موجه به نظر می‌رسد.

علاوه بر این موضوع در هفته گذشته یک بروزرسانی ضروری برای مرورگر کروم[7] منتشر گردید. موضوعی که شرکت گوگل آن را بسیار پراهمیت دانسته و از همه کاربران مربوطه بروزرسانی سریع را تقاضا کرده است. علت اصلی این موضوع وجود یک نقص آزادسازی مجدد حافظه در مرورگر گوگل کروم عنوان شده است. آزادسازی بیش از یکبار حافظه امکان بازنویسی اشاره‌گرهای لیست‌پیوندی[8] فضاهای خالی را ممکن می‌سازد. امری که می‌تواند اجرای کدهای غیرمجاز و حملات انکار سرویس[9] را به دنبال داشته باشد.

آخرین خبر هفته گذشته نیز به آسیب‌پذیری ابزار مشهور پی.اِچ.پی.مای اَدمین[10] در برابر حملات جعل درخواست فرا وبگاهی[11] مربوط می‌گردد. در این حملات به علت عدم رعایت نکات امنیتی هنگام برنامه‌نویسی امکان جعل درخواست‌ها با هدایت قربانی به یک پیوند یا صفحه وب مخرب وجود دارد.

محمد پیشدار

1- Mining is the process of adding transaction records to Bitcoin's public ledger of past transactions and a "mining rig" is a colloquial metaphor for a single computer system that performs the necessary computations for "mining".
2- Malware is any software intentionally designed to cause damage to a computer, server, client or network
3- A central processing unit (CPU) is an important part of every computer
4- A GPU, or Graphics Processing Unit, is a special stream processor used in computer graphics hardware.
5-Skidmap
6- A rootkit is a collection of computer software, typically malicious, designed to enable access to a computer or an area of its software that is not otherwise allowed, and often masks its existence or the existence of other software.
7- Google Chrome is a cross-platform web browser developed by Google.
8- A linked list is a linear data structure where each element is a separate object.
10-phpMyAdmin is a free and open source administration tool for MySQL and MariaDB.
11- Cross-site request forgery or XSRF, is a type of malicious exploit of a website where unauthorized commands are transmitted from a user that the web application trusts.

فهرست مطالب

نمای کلی :

در جدول زیر اطلاعات اخبار هفته گذشته آورده شده است.

انتشار وصله امنیتی ضروری برای مرورگر گوگل‌کُروم	
دستگاه‌های تحت تاثیر	مرورگر گوگل کُروم سیستم‌عامل ویندوز، مَک و لینوکس (نسخه‌های قبل از ۷۷,۰,۳۸۶۵,۹۰)
راه‌های نفوذ	هدایت قربانی به یک صفحه وب مخرب در مرورگر گوگل کُروم
اهداف مهاجمان	اجرای کُدهای غیرمجاز، حملات انکار سرویس، سرقت اطلاعات و تخریب حافظه
کشف بدافزار استخراج ارز دیجیتال در سیستم‌عامل لینوکس[1]	
دستگاه‌های تحت تاثیر	سیستم‌عامل لینوکس
راه‌های نفوذ	دستکاری ماژول امنیتی لینوکس، جایگزینی ماژول احراز هویت لینوکس با یک نسخه مخرب
اهداف مهاجمان	استخراج غیرمجاز ارز دیجیتال
کشف آسیب‌پذیری روز صفر[2] در ابزار پی.اِچ.پی.مای اَدمین	
دستگاه‌های تحت تاثیر	ابزار پی.اِچ.پی مای اَدمین (نسخه ۴,۹,۰۱ ، ۵,۰,۰ آلفا [3]۱ و قبل از آن)
روش نفوذ	حمله جعل درخواست فراوبگاهی
اهداف مهاجمان	حذف پیکربندی خدمات‌رسان در صفحه تنظیمات پَنِل پی.اِچ.پی مای اَدمین

[1]-Linux is a family of free and open-source software operating systems based on the Linux kernel.
[2]-A zero-day (also known as 0-day) vulnerability is a computer-software vulnerability that is unknown to those who would be interested in mitigating the vulnerability (including the vendor of the target software).
[3]-phpMyAdmin 5.0.0-alpha1

خبر شماره ۱ تاریخ انتشار : ۹۸/۰۷/۰۱

انتشار وصله امنیتی ضروری برای مرورگر گوگل‌کُروم

خلاصه

اخیرا شرکت گوگل یک بروزرسانی فوری برای مرورگر گوگل کروم منتشر کرده و از کاربران خود خواسته تا مرورگرهای سیستم‌عامل ویندوز، مَک[1] و لینوکس[2] خود را در اسرع وقت بروزرسانی نمایند. طبق اعلام این شرکت عدم انجام بروزرسانی مربوطه با توجه به شدت خطر می‌تواند هزینه سنگینی را برای کاربران مرورگر کروم به همراه داشته باشد.

برای مشاهده متن کامل خبر می‌توانید به آدرس زیر مراجعه نمایید.

https://cert.ikiu.ac.ir/news-view.php?nid=381

مرجع اصلی خبر

The Hacker News Website

https://thehackernews.com/2019/09/google-chrome-update.html

[1]-macOS is a series of graphical operating systems developed and marketed by Apple Inc. since 2001.
[2]-Linux is a family of free and open-source software operating systems based on the Linux kernel.

خبر شماره ۲ تاریخ انتشار : ۹۸/۰۷/۰۲

کشف بدافزار[1] استخراج ارز دیجیتال در سیستم‌عامل لینوکس

خلاصه

محققان حوزه امنیت اطلاعات موفق به کشف یک بدافزار جدید در سیستم‌عامل لینوکس شده‌اند. این بدافزار اِسکیدمَپ[2] نام داشته و فعالیت‌های خود در زمینه استخراج ارز دیجیتال را با جعل ترافیک شبکه و آمارهای مربوط به پردازنده مخفی نگه می‌دارد. اِسکیدمَپ علاوه بر استخرج ارز دیجیتال، دسترسی بدون وقفه به یک سیستم آلوده را نیز در اختیار مهاجم قرار می‌دهد.

برای مشاهده متن کامل خبر می‌توانید به آدرس زیر مراجعه نمایید.

https://cert.ikiu.ac.ir/news-view.php?nid=382

مرجع اصلی خبر:

Zdnet Website

https://www.zdnet.com/article/skidmap-malware-buries-into-the-kernel-to-hide-cryptocurrency-mining/

[1]-Malware is any software intentionally designed to cause damage to a computer, server, client, or computer network.
[2]-Skidmap

خبر شماره ۳ تاریخ انتشار : ۹۸/۰۷/۰۳

کشف آسیب‌پذیری روز صفر در ابزار پی.اِچ.پی.مای اَدمین

خلاصه

اخیرا محققان امنیت سایبری جزئیات وجود یک آسیب‌پذیری روز صفر را در نرم‌افزار پی.اِچ.پی مای اَدمین به صورت اثبات مفهومی (پی.اُ.سی[۱]) منتشر کرده‌اند. پی.اچ.پی مای اَدمین به عنوان یک نرم‌افزار متن‌باز (زبان برنامه‌نویسی پی.اِچ.پی[۲]) برای مدیریت پایگاه‌های داده مای‌اِسکیوال[۳] شناخته می‌شود. مدیران با استفاده از این ابزار می‌توانند اقداماتی از جمله اجرای عبارات اِسکیوِال[۴]، مدیریت کاربران، تغییر یا حذف جداول، فیلدها و ردیف‌های پایگاه‌داده را انجام دهند. یک مهاجم با وجود این آسیب‌پذیری می‌تواند پیکربندی خدمات‌رسان‌های آسیب‌پذیر را در صفحه تنظیمات پَنِل پی.اِچ.پی مای اَدمین حذف کند.

برای مشاهده متن کامل خبر می‌توانید به آدرس زیر مراجعه نمایید.

https://cert.ikiu.ac.ir/news-view.php?nid=383

مرجع اصلی خبر:

The Hacker News Website

https://thehackernews.com/2019/09/phpmyadmin-csrf-exploit.html?m=1

۱-Proof of concept (PoC) is a realization of a certain method or idea in order to demonstrate its feasibility, or a demonstration in principle with the aim of verifying that some concept or theory has practical potential.

2-PHP: Hypertext Preprocessor is a general-purpose programming language originally designed for web development.

3-MySQL is an open-source relational database management system.

4-SQL is a domain-specific language used in programming and designed for managing data held in a relational database management system, or for stream processing in a relational data stream management system.