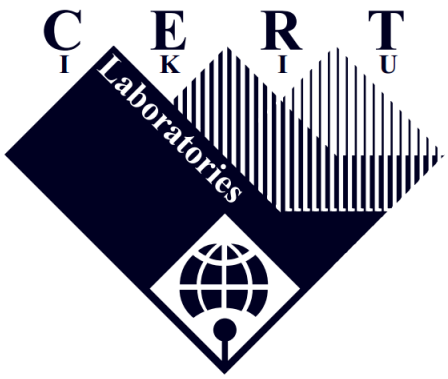

آزمایشگاه تخصصی آپا، قزوین

دانشگاه بین المللی امام خمینی (ره)

هفته نامه تحلیلی رویدادهای امنیتی

شنبه هجدهم خرداد ماه ۱۳۹۸

نسخه ۱,۰,۰

بنام خداوند بخشنده و مهربان

یادداشت سردبیر

در هفته گذشته اخبار متنوعی در حوزه امنیت اطلاعات منتشر گردید. موضوعاتی که دامنه‌ی گسترده‌ای را از پروتکل[1]های شبکه‌های کامپیوتری تا نرم‌افزارها و سیستم‌های‌عامل شامل می‌گردند. یکی از جالب‌ترین این موضوعات کشف آسیب‌پذیری روز صفر در ابزار نوت.پَد[2] بوده است. ابزاری مشهور برای ویرایش فایل‌های متنی در سیستم عامل ویندوز که به علت یک نقص حافظه امکان اجرای کدهای غیرمجاز را برای مهاجمان فراهم می‌سازد. جذابیت این خبر به روش نفوذ یا علت فنی آن مربوط نبوده و تنها به گزارش آسیب‌پذیری مذکور اختصاص دارد. مدتی پس از گزارش این آسیب‌پذیری به مدیران مایکروسافت[3] شرکتی دیگر در حوزه امنیت سایبری، تازگی این نقص را زیر سوال برد. بنا بر اعلام این شرکت نقص مذکور مدت‌ها پیش در حال استفاده توسط مهاجمان سایبری بوده و تنها اخیرا به شرکت ماکروسافت گزارش شده است. این موضوع یکی از حقیقت‌های تلخ دنیای سایبری امروز محسوب می‌گردد. در واقع امروزه در کنار محققان امنیت اطلاعات و آزمایشگاه‌های وابسته یک بازار خرید و فروش اِکسپلویت[4]های آسیب‌پذیری نیز در فضای مجازی شکل گرفته است. این فضا وب تاریک[5] نام داشته که به راحتی توسط پلیس سایبری قابل ردیابی نیست. در این محیط نحوه استفاده از نقص‌های امنیتی قبل از کشف توسط شرکت‌های سازنده با قیمت‌های بسیار بالا به فروش می‌رسد.

علاوه بر این موضوع یکی دیگر از حقایق تلخ حوزه سایبری در هفته گذشته مشاهده می‌شود. با توجه به عناوین اخبار هفته گذشته در سال ۲۰۱۶ یک حمله سایبری موفق به ابزار تیم‌ویوِر[6] صورت گرفته که تا امروز صحت آن توسط مدیران این شرکت کتمان شده است. این افراد بالاخره در هفته گذشته پس از گذشت سه سال به این موضوع اقرار کردند. به طور کلی در بسیاری از مواقع شرکت‌ها برای عدم انتشار اخبار منفی (به ویژه در حوزه امنیت محصولات) نسبت به محصولات خود بسیاری از حقایق را کتمان کرده حتی اگر با این کار به بسیاری از کاربران آسیب برسانند.

محمد پیشدار

[1] In telecommunication, a communication protocol is a system of rules that allow two or more entities of a communications system to transmit information via any kind of variation of a physical quantity.

[2]-Notepad is a simple text editor for Microsoft Windows and a basic text-editing program which enables computer users to create documents.

[3] Microsoft Corporation is an American multinational technology company with headquarters in Redmond, Washington.

[4] An exploit is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug or vulnerability to cause unintended or unanticipated behavior to occur on computer software, hardware, or something electronic (usually computerized).

[5] The dark web is the World Wide Web content that exists on darknets, overlay networks that use the Internet but require specific software, configurations, or authorization to access.

[6] TeamViewer is proprietary software for remote control, desktop sharing, online meetings, web conferencing and file transfer between computers.

فهرست مطالب

نمای کلی :

در جدول زیر اطلاعات اخبار هفته گذشته آورده شده است.

کشف حمله سایبری به تیم‌ویور در سال ۲۰۱۶	
دستگاه‌های تحت تاثیر	نرم‌افزار تیم‌ویور
راه‌های نفوذ	حملات زنجیره تامین و بدافزارهای درب‌پشتی (تروجان ویتنی[1])
اهداف مهاجمان	کنترل از راه دور رایانه قربانیان، سرقت اطلاعات مشتریان
نفوذ به هزاران خدمت‌دهنده پی.اچ.پی‌مای‌اَدمین[2] و اِم.اِس-اس.کیو.اِل[3]	
دستگاه‌های تحت تاثیر	خدمت‌دهندگان پی.اِچ.پی‌مای‌اَدمین و اِم.اِس-اِس.کیو.اِل
روش نفوذ	آسیب‌پذیری افزایش امتیاز، حمله جست‌وجو فراگیر
اهداف مهاجمان	استخراج ارز دیجیتال
نقص جدید در پروتکل آر.دی.پی[4]	
دستگاه‌های تحت تاثیر	سیستم‌عامل ویندوز۷، ایکس.پی ویندوز سرور (۲۰۰۳ و ۲۰۰۸)
روش نفوذ	ارسال درخواست‌های مخرب پروتکل آر.دی.پی
اهداف مهاجمان	اجرای کُدهای دلخواه و غیرمجاز از راه دور
آسیب‌پذیری روز صفر[5] در ابزار نوت.پَد	
دستگاه‌های تحت تاثیر	نوت.پَد ویندوز
روش نفوذ	اجرای یک قطعه کُد پوسته[6] در محیط خط فرمان نوت.پَد، خرابی حافظه
اهداف مهاجمان	اجرای کُدهای دلخواه و غیرمجاز از راه دور

[1] Winnti is a Trojan horse that opens a back door on the compromised computer.

[2] PhpMyAdmin is a free and open source administration tool for MySQL and MariaDB. As a portable web application written primarily in PHP, it has become one of the most popular MySQL administration tools, especially for web hosting services.

[3] MS-SQL: Microsoft SQL Server is a relational database management system developed by Microsoft.

[4] Remote Desktop Protocol (RDP) is a proprietary protocol developed by Microsoft, which provides a user with a graphical interface to connect to another computer over a network connection.

[5]-A zero-day vulnerability is a computer-software vulnerability that is unknown to those who would be interested in mitigating the vulnerability. Until the vulnerability is mitigated, hackers can exploit it to adversely affect computer programs, data, additional computers or a network.

[6]-In computing, a shell is a user interface for access to an operating system's services.

خبر شماره ۱ تاریخ انتشار : ۹۸/۰۳/۱۱

کشف حمله سایبری به تیم‌ویوِر در سال ۲۰۱۶

خلاصه

تیم‌ویوِر یکی از محبوب‌ترین نرم‌افزارها در جهان بوده که به کاربران اجازه دسترسی و اشتراک‌گذری (از راه دور) صفحه نمایش رایانه‌ها را می‌دهد. به گفته روزنامه آلمانی دِراِشپیگِل[1] (۱۷ مه ۲۰۱۹) این نرم‌افزار در سال ۲۰۱۶ مورد حمله سایبری خطرناکی قرار گرفته است. حمله‌ای که در آن مهاجمان به توانایی کنترل رایانه‌های قربانی (بدون اطلاع آنان) از راه دور رسیده‌اند. البته به اذعان شرکت تیم‌ویوِر تا کنون هیچ مدرکی مبنی بر سرقت اطلاعات مشتریان یافت نشده است.

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

https://cert.ikiu.ac.ir/news-view.php?nid=299

مرجع اصلی خبر:

TheHackerNews Website

https://thehackernews.com/2019/05/teamviewer-software-hacked.html?m=1

[1] Der Spiegel is a German weekly news magazine published in Hamburg. With a weekly circulation of 840,000 copies, it is the largest such publication in Europe.

خبر شماره ۲ تاریخ انتشار : ۹۸/۰۳/۱۱

نفوذ به هزاران خدمت‌دهنده پی.اِچ.پی‌مای‌اَدمین و اِم.اِس-اس.کیو.اِل

خلاصه

۲۹ مه ۲۰۱۹ محققان گروه تحقیقاتی «گاردی‌کورلَبس»[1] گزارش مفصلی را درباره عملیات گسترده استخراج ارز دیجیتال[2] در حمله به خدمت‌دهندگان[3] پی.اِچ.پی‌مای‌اَدمین و اِم.اِس-اِس.کیو.اِل منتشر کردند. این عملیات مخرب با نام «نانشو»[4] شناخته شده و توسط گروهی از نفوذگران ای.پی.تی[5] چینیِ برنامه‌ریزی و اجرا می‌شود. در حال حاضر حدود ۵۰۰۰۰ سرویس‌دهنده توسط این گروه با بدافزارهای روت‌کیت[6] آلوده شده است.

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

https://cert.ikiu.ac.ir/news-view.php?nid=300

مرجع اصلی خبر

TheHackerNews Website

https://thehackernews.com/2019/05/hacking-mysql-phpmyadmin.html?m=1

[1] Guardicore Labs is a global research team, consisting of hackers, cybersecurity researchers and industry experts.
[2] Cryptojacking is the secret use of your computing device to mine cryptocurrency.
[3] In computing, a server is a computer program or a device that provides functionality for other programs or devices, called "clients".
[4] The Nansh0u campaign is not a typical crypto-miner attack. It uses techniques often seen in advanced persistent threats (APTs) such as fake certificates and privilege escalation exploits.
[5] An advanced persistent threat (APT) is a stealthy computer network attack in which a person or group gains unauthorized access to a network and remains undetected for an extended period.
[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 (for example, to an unauthorized user) and often masks its existence or the existence of other software.

خبر شماره ۳ تاریخ انتشار : ۹۸/۰۳/۱۲

نقص جدید در پروتکل آر.دی.پی

خلاصه

پس از ارائه وصله امنیتی شرکت مایکروسافت[1] در ماه مِی ۲۰۱۹، نقصی تحت عنوان بِلوکیپ در نسخه‌های قدیمی ویندوز افشا شد. نقصی که مهاجمان با وجود آن می‌توانند از طریق سرویس آر.دی.پی ویندوز بدافزارها[2] را مانند یک کرم[3] در سیستم قربانی منتشر کنند. البته این مشکل چندی قبل با ارائه وصله جدیدی توسط مایکروسافت در ویندوزهای ایکس.پی، ۷، سرور ۲۰۰۳ و ۲۰۰۸ رفع شده است.

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

https://cert.ikiu.ac.ir/news-view.php?nid=301

مرجع اصلی خبر:

Zdnet Website

https://www.zdnet.com/article/almost-one-million-windows-systems-vulnerable-to-bluekeep-cve-2019-0708/

[1]-Microsoft Corporation (MS) is an American multinationaltechnology companywith headquarters in Redmond, Washington. It develops, manufactures, licenses, supports and sells computer software, consumer electronics, personal computers, and related services.

[2]-Ransomware is a type of malicious software from cryptovirology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.

[3]-A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers.

خبر شماره ۴ تاریخ انتشار : ۹۸/۰۳/۱۵

آسیب‌پذیری روز صفر در ابزار نوت.پَد

خلاصه

نوت.پَد ابزاری رایج و مشهور در سیستم‌عامل ویندوز برای نگارش، ویرایش و ذخیره‌سازی متن‌ها است. اخیرا محققان حوزه امنیت اطلاعات یک آسیب‌پذیری روز صفر را در این ابزار کشف کرده‌اند. نوعی نقص حافظه[1] که در صورت بهره‌گیری صحیح آن می‌توان به اجرای کُدهای دلخواه بر روی رایانه‌های آسیب‌پذیر رسید. در این خرابی عموما به علت خطای برنامه‌نویسی ابتدا محتوای حافظه تخریب شده و سپس دوباره مورد استفاده قرار می‌گیرد.

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

https://cert.ikiu.ac.ir/news-view.php?nid=302

مرجع اصلی خبر:

Threatpost Website

https://threatpost.com/researcher-exploits-microsofts-notepad-to-pop-a-shell/145242/

[1]-Memory corruption occurs in a computer program when the contents of a memory location are modified due to programmatic behavior that exceeds the intention of the original programmer or program/language constructs. this is termed violating memory safety.