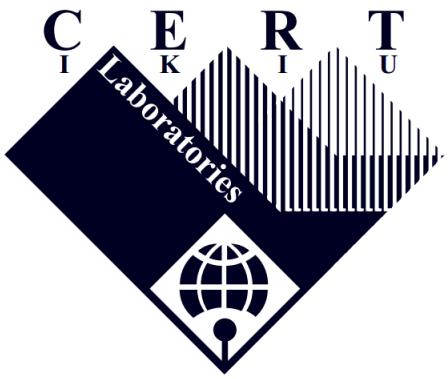

آزمایشگاه تخصصی آپا، قزوین

دانشگاه بین المللی امام خمینی (ره)

هفته نامه تحلیلی رویدادهای امنیتی

شنبه بیست و چهارم فروردین ماه ۱۳۹۸

نسخه ۱,۰,۰

بنام خداوند بخشنده و مهربان

یادداشت سردبیر

نقص فنی در فرآیند اعتبارسنجی بخش‌های مختلف یک سیستم اساسی‌ترین مشکل امنیتی هفته گذشته بوده است. سیستم‌های آسیب‌پذیر در هفته گذشته (که عموما از مسیریاب‌ها تشکیل شده‌اند) به نوعی تحت تاثیر فرآیند اعتبارسنجی نادرست هنگام ورود کاربران و یا درخواست منابع از سیستم‌های خارجی قرار گرفته‌اند. در یکی از اخبار هفته گذشته به علت ضعف فرآیند رمزنگاری هنگام اعتبارسنجی کاربران سرقت اطلاعات مهمی نظیر نام‌های کاربری و کلمات عبور در برخی مسیریاب[۱]های سیسکو[۲] ممکن است. در یک خبر دیگر برنامه مدیریت سیستم مدیریت محتوای وُردپِرس[۳] مبتنی بر آی.اُ.اِس[۴] هنگام درخواست تصاویر موجود در منابع خارجی (نظیر وبگاه‌های اشتراک تصویر) نشانه‌های دسترسی محرمانه[۵] را نیز ارسال می‌کند. فرآیندی که اطلاعات مهم و محرمانه را در اختیار وبگاه‌های مذکور نیز قرار می‌دهد. رویکرد اعتبارسنجی جدید شرکت فیسبوک[۶] در هفته گذشته نیز در این دسته جای خواهد گرفت. در این روش از صاحبان حساب‌های کاربری مشکوک درخواست ارسال کلمات عبور پست‌های الکترونیکی جهت تایید آن شده است. لازم به ذکر است که شرکت فیسبوک در سال گذشته تحت فشار گسترده افکار عمومی برای موضوع اشتراک غیرمجاز اطلاعات کاربران با شرکای خود قرار داشت. احتمالا این نقص امنیتی جدید نیز بر این امر بیافزاید.

علاوه بر اعتبارسنجی ناصحیح عدم مدیریت صحیح حافظه نیز در اخبار هفته گذشته مشاهده می‌گردد. برخی مسیریاب‌های میکروتِک[۷] در هفته گذشته هنگام دریافت بسته‌های آی.پی[۸] نسخه ۶ با پارامترهای خاص واکنش مناسبی از خود نشان نداده و گاهی اوقات در شرایط انکار سرویس[۹] قرار می‌گیرند. سال گذشته نیز مسیریاب‌های میکروتک به علت نقص امنیتی در مولفه وینباکس[۱۰] مورد هجوم گسترده مهاجمان قرار گرفتند.

محمد پیشدار

---

[1] A router is a networking device that forwards data packets between computer networks

[2] Cisco Systems, Inc. is an American multinational technology conglomerate headquartered in San Jose, California.

[3] WordPress is a free and open-source content management system based on PHP & MySQL.

[4] iOS is a mobile operating system created and developed by Apple Inc.

[5] In computer systems, an access token contains the security credentials for a login session and identifies the user, the user's groups, the user's privileges, and, in some cases, a particular application

[6] Facebook, Inc. is an American online social media and social networking service company.

[7] MikroTik is a Latvian company which was founded in 1996 to develop routers and wireless ISP systems

[8] The Internet Protocol (IP) is the principal communications protocol in the Internet protocol suite for relaying datagrams across network boundarie

[9] Denial-of-service attack (DoS attack) is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet.

[10] In computer systems, an access token contains the security credentials for a login session and identifies the user, the user's groups, the user's privileges, and, in some cases, a particular application

فهرست مطالب

نمای کلی :

در جدول زیر اطلاعات اخبار هفته گذشته آورده شده است.

رفع دو آسیب‌پذیری مهم در مسیریاب‌های سیسکو	
دستگاه‌های تحت تاثیر	مسیریاب‌های وَن وی.پی.اِن دوگیگابیتی[1] آر.وی۳۲۰، آر.وی۳۲۵
راه‌های نفوذ	حمله مردمیانی[2] ، فرآیند تحلیل رمز[3] در اعتبارسنجی کاربران دستگاه‌های آسیب‌پذیر، هدایت قربانی به یک وبگاه جعلی از طریق مهندسی اجتماعی[4]
اهداف مهاجمان	اجرای کُدهای دلخواه و غیرمجاز ، افشای اطلاعات مهم سیستمی نظیر نام کاربری و کلمه عبور، دسترسی به اطلاعات حساس مبتنی بر مرورگر
آسیب‌پذیری انکار سرویس دربرخی مسیریاب‌های میکروتِک	
دستگاه‌های تحت تاثیر	مسیریاب‌های میکروتِک
راه‌های نفوذ	ارسال بسته‌های خاص پروتکل آی.پی نسخه‌ی ۶ [5] به مسیریاب قربانی
اهداف مهاجمان	ایجاد شرایط انکار سرویس
نقص امنیتی در برنامه مدیریت وُردپِرس مبتنی بر آی.اُ.اِس	
دستگاه‌های آسیب‌پذیر	برنامه وُردپرس مبتنی بر آس.اُ.اِس
روش نفوذ	سوءاستفاده از ارسال نشانه‌های دسترسی محرمانه هنگام در خواست تصاویر موجود در میزبان‌های خارجی در وُردپرس مبتنی بر آی.اُ.اِس
اهداف مهاجمان	اشتراک‌گذاری «نشانه‌های احراز هویت محرمانه» حساب مدیریت در وبگاه‌های شخص ثالث
درخواست فِیسبوک از کاربران خود برای ارائه رمزعبور پست‌های الکترونیکی	
دستگاه‌های آسیب‌پذیر	شبکه‌اجتماعی فِیسبوک
روش نفوذ	درخواست رمز عبور پست‌های الکترونیکی شخصی در فرآیند احراز هویت جدید فِیسبوک
اهداف مهاجمان	افشای رمزعبور پست‌الکترونیکی کاربران

[1] Dual Gigabit WAN VPN Router

[2] In cryptography and computer security, a man-in-the-middle attack (MITM) is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.

[3] Cryptanalysis is the study of analyzing information systems in order to study the hidden aspects of the systems

[4] Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information

[5] Internet Protocol version 6 (IPv6) is the most recent version of the Internet Protocol (IP), the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet

خبر شماره ۱ تاریخ انتشار : ۹۸/۰۱/۱۹

رفع دو آسیب‌پذیری مهم در مسیریاب‌های سیسکو

خلاصه

اخیرا شرکت سیسکو به منظور رفع دو آسیب‌پذیری بحرانی در مسیریاب‌های آر.وی۳۲۰[1] و آر.وی۳۲۵[2] وصله[3] امنیتی منتشر کرده است. در این بروزرسانی علی‌رغم رفع دو آسیب‌پذیری بحرانی دو نقص مهم نیز بدون واکنش باقی مانده‌اند. این دو مسیریاب در میان شرکت‌های مجری خدمات اینترنتی و هدایت ترافیک شبکه محبوبیت زیادی دارند.

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

https://cert.ikiu.ac.ir/news-view.php?nid=254

مرجع اصلی خبر:

Threatpost Website

https://threatpost.com/cisco-finally-patches-routers-bugs-as-new-unpatched-flaws-surface/143528/

[1] RV320
[2] RV325
[3] A patch is a set of changes to a computer program or its supporting data designed to update, fix, or improve it

خبر شماره ۲ تاریخ انتشار : ۹۸/۰۱/۲۰

آسیب‌پذیری انکار سرویس[1] دربرخی مسیریاب[2]های میکروتِک[3]

میکروتِک یک شرکت مشهور و جهانی در زمینه ارائه خدمات اینترنتی[4] و تولید مسیریاب‌ها است. اخیرا مسیریاب‌های این شرکت تحت تاثیر آسیب‌پذیری خطرناکی از دسته انکار سرویس (دی.اُ.اِس) قرار گرفته‌اند. نقص که در صورت بهره‌گیری صحیح می‌تواند سیستم قربانی را راه‌اندازی مجدد کرده و باعث اختلال در عملکرد خدمات‌رسان‌ها[5] گردد.

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

https://cert.ikiu.ac.ir/news-view.php?nid=256

مرجع اصلی خبر

Bleeping Computer Website

https://www.bleepingcomputer.com/news/security/year-old-dos-vulnerability-allows-attacks-on-some-mikrotik-routers/

[1]Denial-of-service attack (DoS attack) is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet.

[2] A router is a networking device that forwards data packets between computer networks

[3] MikroTik is a Latvian company which was founded in 1996 to develop routers and wireless ISP systems

[4] An Internet service provider (ISP) is an organization that provides services for accessing, using, or participating in the Internet.

[5] In computing, a server is a computer program or a device that provides functionality for other programs or devices, called "clients".

خبر شماره ۳ تاریخ انتشار : ۹۸/۰۱/۲۰

نقص امنیتی در برنامه مدیریت وُردپِرِس[1] مبتنی بر آی.اُ.اِس[2]

خلاصه

اخیرا وُردپرس یک آسیب‌پذیری شدید در برنامه مبتنی بر سیستم‌عامل آی.اُ.اِس را وصله کرده است. در این آسیب پذیری «نشانه‌های احراز هویت محرمانه» کاربران برنامه وُردپرس مبتنی بر آی.اُ.اِس می‌تواند برای وبگاه‌های خارجی افشا گردد. در واقع خود برنامه وُردپرس مبتنی بر آی.اُ.اِس در شرایطی خاص نشانه‌های دسترسی را برای وبگاه‌های مذکور ارسال می‌کند.

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

https://cert.ikiu.ac.ir/news-view.php?nid=257

مرجع اصلی خبر:

TheHackerNews Website

https://thehackernews.com/2019/04/wordpress-ios-security.html?m=1

[1] WordPress is a free and open-source content management system based on PHP & MySQL. Features include a plugin architecture and a template system. It is most associated with blogging but supports other types of web content including more traditional mailing lists and forums, media galleries, and online stores.

[2] iOS is a mobile operating system created and developed by Apple Inc. exclusively for its hardware. It is the operating system that presently powers many of the company's mobile devices, including the iPhone, iPad, and iPod Touch.

خبر شماره ۴ تاریخ انتشار : ۹۸/۰۱/۲۲

درخواست فِیسبوک از کاربران خود برای ارائه رمزعبور پست‌های الکترونیکی

خلاصه

اخیرا وُردپرس یک آسیب‌پذیری شدید در برنامه مبتنی بر سیستم‌عامل آی.اُ.اِس را وصله کرده است. در این آسیب پذیری «نشانه‌های احراز هویت محرمانه» کاربران برنامه وُردپرس مبتنی بر آی.اُ.اِس می‌تواند برای وبگاه‌های خارجی افشا گردد. در واقع خود برنامه وُردپرس مبتنی بر آی.اُ.اِس در شرایطی خاص نشانه‌های دسترسی را برای وبگاه‌های مذکور ارسال می‌کند.

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

https://cert.ikiu.ac.ir/news-view.php?nid=258

مرجع اصلی خبر:

TheHackerNews Website

https://thehackernews.com/2019/04/facebook-email-password.html?m=1