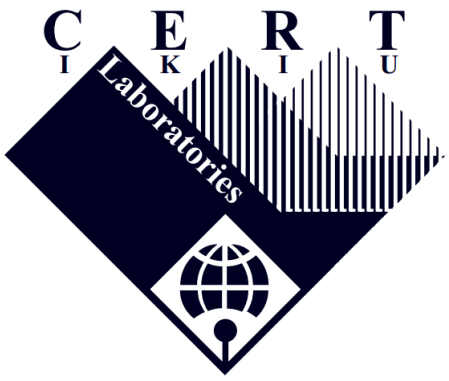

آزمایشگاه تخصصی آپا، قزوین

دانشگاه بین المللی امام خمینی (ره)

هفته نامه تحلیلی رویدادهای امنیتی

شنبه بیست و هفتم مهر ماه ۱۳۹۸

نسخه ۱,۰,۰

بنام خداوند بخشنده و مهربان

یادداشت سردبیر

معمولا بسیاری از فناوری‌ها در دنیای رایانش و الکترونیک با یکدیگر اشتراکات قابل توجهی دارند. به عنوان مثال در بسیاری از دستگاه‌های تولید یک شرکت، خانواده یکسانی از تراشه‌ها، سیستم‌عامل[۱] و یا حتی نرم‌افزارها استفاده می‌شوند. گاهی اوقات چندین نماد تجاری در حوزه‌های مذکور با یکدیگر همکاری کرده و بر این اساس حجم اشتراکات از سطح یک شرکت نیز فراتر می‌رود. این موضوع در برخی مواقع خاص می‌تواند از جنبه رایانش امن بسیار خطرناک باشد. در واقع اشتراکات همان اندازه که در توسعه فناوری موثر هستند می‌توانند هنگام کشف یک نقص امنیتی مضر باشند. به عبارت دیگر کشف یک آسیب‌پذیری در سطح بالاتری از این اشتراکات متناظر با نفوذ یا تخریب بخش بزرگتری از تجهیزات و سیستم‌های مربوطه است.

در چندین هفته اخیر این موضوع چهره قابل توجهی را در بین اخبار امنیتی پیدا کرده است. تنها در هفته گذشته یک نقص بحرانی دو تراشه ساخت شرکت‌های اینتِل[۲] و اِنویدیا[۳] را تحت تاثیر قرار می‌دهد. نقصی که با توجه به کاربرد این دو تراشه در بسیاری از ابزارهای الکترونیکی نظیر تلویزیون‌های اِنویدیا شیلد (نسخه ۸,۰,۱ و قبل از آن) و رایانه‌های کوچک اینتِل اِن.یو.سی (شامل کیت بازی اصلی اِن.یو.سی۸[۴]) طیف گسترده‌ای از دستگاه‌های آسیب‌پذیر را تهدید خواهد کرد. دو خبر دیگر هفته گذشته نیز به نوعی با این موضوع در ارتباط هستند. در خبر اول کشف یک آسیب‌پذیری سرقت دی.اِل.اِل[۵] در سرویس‌های تحلیل فرامین لمسی[۶] اِچ.پی[۷] بسیاری از رایانه‌های شخصی این شرکت را در خطر اجرای کدهای غیرمجاز قرار داده و در دومین خبر این اتفاق با کشف یک آسیب‌پذیری روز صفر[۸] در برنامه‌های آیتونز[۹] و آیکلود[۱۰] تکرار می‌شود.

---

[1]-An operating system (OS) is system software that manages computer hardware, software resources, and provides common services for computer programs.

[2]-Intel Corporation is an American multinational corporation and technology company headquartered in Santa Clara, California, in the Silicon Valley.

[3]-Nvidia Corporation is an American technology company incorporated in Delaware and based in Santa Clara, California.

[4]-NUC 8 mainstream game kit

[5]-DLL Hijacking is an attack that exploits the way some Windows applications search and load Dynamic Link Libraries. Most Windows applications will not use a fully qualified path to load any required DLLs. A Attacker can place a fake DLL for a known program in a location that is searched before the real DLL's location and almost guarantee that the malicious DLL is loaded, resulting in whatever code the attacker wants to run running!

[6]-HP TouchPoint Analytics is a service that anonymously collects diagnostic information about hardware performance.

[7]-The Hewlett-Packard Company or Hewlett-Packard was an American multinational information technology company headquartered in Palo Alto, California.

[8]-A zero-day vulnerability is a computer-software vulnerability that is unknown to those who would be interested in mitigating the vulnerability

[9]-iTunes is a media player, media library, Internet radio broadcaster, and mobile device management application developed by Apple Inc.

[10]-iCloud is a cloud storage and cloud computing service from Apple Inc.

موضوعی بدون جزئیات که تنها از آسیب‌پذیری رایانه‌های ویندوز بسیاری نسبت به اجرای کدهای غیرمجاز خبر می‌دهد. چرا که این نقص تنها مربوط به نسخه ویندوز ابزارهای مذکور است.

با توجه به این موارد بدیهی است که بسیاری از مهاجمان سایبری علاقه بیشتری نسبت به کشف آسیب‌پذیری در سطوح بالای سیستم‌های دارای اشتراکات فراوان داشته باشند. لذا انتخاب سرمایه‌گذاری امنیتی مناسب برای مقابله با این تهدیدات در مقابل ضرر ناشی از آن کاری بسیار عقلانی است.

محمد پیشدار

فهرست مطالب

نمای کلی :

در جدول زیر اطلاعات اخبار هفته گذشته آورده شده است.

نقص امنیتی در سرویس‌های تحلیل فرامین لمسی اِچ.پی	
دستگاه‌های تحت تاثیر	رایانه‌های شخصی اِچ.پی
راه‌های نفوذ	سرقت دی.اِل.اِل[1]
اهداف مهاجمان	اجرای کدهای دلخواه در سطح کاربر قربانی
آسیب‌پذیری روز صفر در برنامه‌های آیتونز و آیکلود	
دستگاه‌های تحت تاثیر	سیستم‌عامل ویندوز دارای برنامه‌های آیتونز و آیکلود
راه‌های نفوذ	سوءاستفاده از یک آسیب‌پذیری روز صفر در سرویس بُنجور[2]
اهداف مهاجمان	اجرای غیرمجاز کدهای دلخواه در سیستم قربانی
نقص امنیتی بحرانی در دو تراشه ساخت شرکت‌های اینتِل و اِنویدیا	
دستگاه‌های تحت تاثیر	تلویزیون‌های اِنویدیا شیلد (نسخه ۸,۰,۱ و قبل از آن) و رایانه‌های کوچک اینتِل اِن.یو.سی شامل کیت بازی اصلی اِن.یو.سی۸، رایانه‌های کوچک بازی، اینتِل اِن.یو.سی بُرد دی.ای۳۸۱۵.تی.وای.بی.ای[3] (مدل ۵۰۰- اِچ۲۶۹۹۸[4] و بعد از آن)، اِن.یو.سی کیت. دی.ای ۳۸۱۵.تی. کا.اِچ.ای [5] (مدل ۵۰۰- اِچ ۲۷۰۰۲[6] و بعد از آن) و اِن.یو.سی کیت دی.اِن ۲۸۲۰ اِف.وای.کا[7]
روش نفوذ	ارسال یک بسته تی.سی.پی[8] مخرب به دستگاه آسیب‌پذیر
اهداف مهاجمان	اجرای کُدهای غیرمجاز، افزایش سطح دسترسی، انکار سرویس و افشای اطلاعات

[1]-DLL Hijacking is an attack that exploits the way some Windows applications search and load Dynamic Link Libraries. Most Windows applications will not use a fully qualified path to load any required DLLs. A Attacker can place a fake DLL for a known program in a location that is searched before the real DLL's location and almost guarantee that the malicious DLL is loaded, resulting in whatever code the attacker wants to run running!

[2]-Bonjour is Apple's implementation of zero-configuration networking, a group of technologies that includes service discovery, address assignment, and hostname resolution.

[3]-the Intel NUC Board DE3815TYBE

[4]-H26998-500

[5]-NUC Kit DE3815TYKHE

[6]-H27002-500

[7]-NUC Kit DN2820FYKH

[8]-The Transmission Control Protocol (TCP) is one of the main protocols of the Internet protocol suite.

خبر شماره ۱ تاریخ انتشار : ۹۸/۰۷/۲۱

نقص امنیتی در سرویس‌های تحلیل فرامین لمسی اِچ.پی

خلاصه

محققان حوزه امنیت اطلاعات موفق به کشف یک آسیب‌پذیری جدید در سرویس تحلیل فرامین لمسی رایانه‌های شخصی اِچ.پی شده‌اند. این آسیب‌پذیری به یک مسئله بارگذاری فایل‌های کتابخانه‌ای دی.اِل.اِل[1] در ابزار نظارت سخت افزار[2] (متن باز) برمی‌گردد. نقصی که بهره‌گیری موفق از آن می‌تواند اجرای کُدهای دلخواه در سطح دسترسی کاربر قربانی را برای مهاجم به ارمغان بیاورد.

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

https://cert.ikiu.ac.ir/news-view.php?nid=398

مرجع اصلی خبر

Threatpost Website

https://threatpost.com/hp-touchpoint-analytics-opens-pcs-to-code-execution-attack/149069/

[1]-Dynamic-link library (DLL) is Microsoft's implementation of the shared library concept in the Microsoft Windows and OS/2 operating systems. These libraries usually have the file extension DLL, OCX, or DRV.

[2]-The Open Hardware Monitor is a free open source software that monitors temperature sensors, fan speeds, voltages, load and clock speeds of a computer. The Open Hardware Monitor supports most hardware monitoring chips found on todays mainboards.

خبر شماره ۲ تاریخ انتشار : ۹۸/۰۷/۲۴

آسیب‌پذیری روز صفر در برنامه‌های آیتونِز و آیکلود

خلاصه

اخیرا گونه جدیدی از باج‌افزار بیت‌پیمِر[1] برخی از رایانه‌های ویندوزی را به وسیله یک آسیب‌پذیری روز صفر مربوط به برنامه‌های آیتونِز (نرم‌افزار پخش فایل‌های صوتی و تصویری در اَپل[2]) و آیکلود (سرویس ابری اَپل) آلوده کرده است. در واقع مهاجمان با آسیب‌پذیری موجود در این دو برنامه توانسته کُدهای مخرب خود را با امضای دیجیتال معتبر در سیستم قربانی اجرا کنند. در این صورت هیچ برنامه‌های ضد ویروسی قادر به شناسایی آن‌ها نخواهد بود.

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

https://cert.ikiu.ac.ir/news-view.php?nid=399

مرجع اصلی خبر:

The Hacker News Website

https://thehackernews.com/2019/10/apple-bonjour-ransomware.html

[1]-Ransom.Bitpaymer is a Trojan horse that encrypts files on the compromised computer and demands a payment to decrypt them.

[2]-Apple Inc. is an American multinational technology company headquartered in Cupertino, California, that designs, develops, and sells consumer electronics, computer software, and online services. It is considered one of the Big Four tech companies along with Amazon, Google, and Facebook.

خبر شماره ۳ تاریخ انتشار : ۹۸/۰۷/۲۴

نقص امنیتی بحرانی در دو تراشه ساخت شرکت‌های اینتِل و اِنویدیا

خلاصه

اخیرا شرکت‌های اینتِل و اِنویدیا دو غول عرصه ساخت پردازنده‌ها اقدام به انتشار یک بروزرسانی برای تلویزیون‌های اِنویدیا شیلد[1] و رایانه‌های کوچک اینتِل اِن.یو.سی[2] کرده‌اند. در این بروزرسانی دو نقص در اِنویدیا شیلد و دو آسیب‌پذیری در اینتِل اِن.یو.سی رفع شده است. نتیجه بهره‌گری از این آسیب‌پذیری‌ها اجرای کُدهای غیرمجاز، افزایش سطح دسترسی، حملات انکار سرویس[3] و افشا اطلاعات عنوان شده است.

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

https://cert.ikiu.ac.ir/news-view.php?nid=400

مرجع اصلی خبر:

Threatpost Website

https://threatpost.com/gamers-high-severity-intel-nvidia-flaws/149034/

[1]-The Nvidia Shield, also known as the Shield Android TV or Shield Console, is an Android TV-based digital media player produced by Nvidia as part of its Shield brand of Android devices.
[2]-Intel Next Unit of Computing mini-PC
[3]-In computing, a 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.