مرکز آپا دانشگاه سمنان

خبرنامه الکترونیکی ۶۹

مرکز تخصصی آپا دانشگاه سمنان

در این شماره می‌خوانید:

آشنایی با پروتکل CDP و بررسی نمونه‌ای از این پروتکل در وایرشارک

شماره شصت و نهم، سال ششم، اسفند ۱۴۰۲ | کاری از تیم تولید محتوای مرکز تخصصی آپا دانشگاه سمنان

https://cert.semnan.ac.ir info.cert@semnan.ac.ir 023-31535019 @semcert

سال ۱۴۰۳ مبارک

مرکز آپا دانشگاه سمنان

فهرست

خبر

آموزش

مرکز آپا دانشگاه سمنان

اخبار امنیت سایبری

کشف آسیب‌پذیری در Microsoft Edge

دو آسیب‌پذیری با شناسه‌های CVE-2024-26192 با شدت بالا (8.2) و CVE-2024-26188 با شدت متوسط (4.3) در Microsoft Edge کشف شده است. با بهره‌برداری از آسیب‌پذیری CVE-2024-26192 که یک نقص Information Disclosure یا افشای اطلاعات است، مهاجم می‌تواند به اطلاعات حساس دسترسی پیدا کند. همچنین با بهره‌برداری از آسیب‌پذیری CVE-2024-26188، مهاجم قادر به اجرای حمله Spoofing یا جعل است و می‌تواند دسترسی غیرمجاز پیدا کند.

- **بردار حمله برای آسیب‌پذیری CVE-2024-26192 :**

بر اساس بردار حمله این آسیب‌پذیری (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:N/A:L) بهره‌برداری از طریق شبکه خارجی و از راه دور امکان‌پذیر است (AV:N)، نیازمند هیچ پیش‌زمینه‌ای نبوده و به راحتی قابل تکرار است و به شرایط خاصی نیازنیست (AC: L)، مهاجم برای انجام حمله نیاز به حساب‌کاربری با سطح دسترسی بالا یا پایین ندارد (PR: N)، به تعامل با کاربر نیز نیاز دارد (UI:R)، بهره‌برداری از نقص امنیتی مذکور بر سایر منابع امنیتی تأثیر می‌گذارد (S:C) و با بهره‌برداری از این آسیب‌پذیری، یک ضلع از سه ضلع امنیت را با شدت بالا تحت تأثیر قرار می‌گیرد.

- **بردار حمله برای آسیب‌پذیری CVE-2024-26188 :**

بر اساس بردار حمله این آسیب‌پذیری (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N) بهره‌برداری از طریق شبکه خارجی و از راه دور امکان‌پذیر است (AV:N)، نیازمند هیچ پیش‌زمینه‌ای نبوده و به راحتی قابل تکرار است و به شرایط خاصی نیازنیست (AC: L)، مهاجم برای انجام حمله نیاز به حساب‌کاربری با سطح دسترسی بالا یا پایین ندارد (PR: N)، به تعامل با کاربر نیز نیاز دارد (UI:R)، بهره‌برداری از نقص امنیتی مذکور بر سایر منابع امنیتی تأثیر نمی‌گذارد (S:U) و با بهره‌برداری از این آسیب‌پذیری، یک ضلع از سه ضلع امنیت را با شدت کم تحت تأثیر قرار می‌گیرد.

توصیه‌های امنیتی

به کاربران توصیه می‌شود مرورگر خود را به آخرین نسخه موجود به‌روزرسانی کنند.

منبع خبر:

https://nvd.nist.gov/vuln/detail/CVE-2024-26192

https://nvd.nist.gov/vuln/detail/CVE-2024-26188

کشف یک تروجان منبع باز به نام Xeno RAT

یک تروجان دسترسی از راه دور (RAT) به نام Xeno RAT در GitHub منتشر شده است. این RAT طوری طراحی شده است که به مهاجمان امکان دسترسی از راه دور به رایانه‌های ویندوز 10 و ویندوز 11 را می‌دهد. این تروجان به زبان #C نوشته شده است و طیف گسترده‌ای از ویژگی‌ها را برای مدیریت سیستم‌ها از راه دور ارائه می‌دهد.

برخی از قابلیت‌های آن عبارتند از:

1. SOCKS5 Reverse Proxy: این قابلیت به مهاجمان اجازه می‌دهد تا ترافیک شبکه خود را از طریق رایانه آلوده هدایت کنند، مکان خود را پنهان کرده و ردیابی فعالیت‌های آن‌ها را دشوارتر می‌کند.
2. ضبط صدا در لحظه: Xeno RAT می‌تواند صدا را از میکروفون کامپیوتر آلوده ضبط کند و به طور بالقوه به مهاجمان اجازه می‌دهد مکالمات را شنود کنند.
3. ماژول محاسبات شبکه مجازی مخفی (hVNC): این ماژول به مهاجمان اجازه می‌دهد تا رابط دسکتاپ رایانه آلوده را از راه دور کنترل کنند و به آن‌ها دسترسی کامل به سیستم قربانی می‌دهد.طبق بررسی های انجام شده این تروجان شامل یک ابزار برای شخصی‌سازی است که به مهاجمان اجازه می‌دهد نسخه‌های بدافزار خود را شخصی‌سازی و آن را متناسب با نیازهای خاص خود تنظیم کنند.

Xeno RAT یک تهدید جدی است زیرا ابزار قدرتمندی برای دسترسی و کنترل از راه دور رایانه‌های ویندوزی در اختیار مهاجمان قرار می‌دهد که به طور بالقوه منجر به دسترسی غیرمجاز، سرقت داده‌ها و سایر فعالیت‌های مخرب می‌شود.

منبع خبر:

https://thehackernews.com/2024/02/open-source-xeno-rat-trojan-emerges-as.html

کشف پنج آسیب‌پذیری در سیستم مدیریت‌محتوای Joomla

پنج آسیب‌پذیری در سیستم مدیریت محتوای Joomla کشف شده است که ممکن است برای اجرای کد دلخواه در وب‌سایت‌های آسیب‌پذیر استفاده شوند. اولین آسیب‌پذیری با شناسه CVE-2024-21722 و شدت 7.5 مربوط به مدیریت احراز هویت دو عاملی[1] است. زمانی که روش‌های MFA یک کاربر تغییر می‌کند، سشن‌های کاربری موجود را به درستی پایان نمی‌دهد که این امر می‌تواند به مهاجمان اجازه دهد تا از سشن‌های فعال قبلی بهره‌برداری کنند.

آسیب‌پذیری دیگری با شناسه CVE-2024-21723 و شدت 9.1 ناشی از تجزیه نادرست URLها است که می‌تواند منجر به یک تغییر مسیر شود و کاربران را به سایت‌های مخرب هدایت کند.

آسیب‌پذیری بعدی با شناسه CVE-2024-21724 و شدت 7.8 نیز یک آسیب‌پذیری‌های از راه دور از نوع XSS است که به مهاجمان اجازه می‌دهد کدهای مخرب را اجرا کنند.

یک آسیب‌پذیری دیگر که شناسه CVE-2024-21725 و شدت 6.3 به آن اختصاص داده شده است منجر به نقص XSS در مؤلفه‌های مختلف می‌شود و مهاجمان می‌توانند از طریق آدرس‌های ایمیل مخرب، کدهای مخرب خود را اجرا می‌کنند.

آخرین آسیب‌پذیری با شناسه CVE-2024-21726 و شدت 7.8 منجر به چندین آسیب‌پذیری XSS می‌شود که مهاجمان می‌توانند از طریق آنها به طور دلخواه کدهای مخرب را در وب‌سایت قربانی اجرا کنند.

محصولات تحت تأثیر

نسخه‌های متاثر از آسیب‌پذیری‌ها عبارتند از:

- Joomla! CMS نسخه‌های 3.2.0 تا 3.10.14
- Joomla! CMS نسخه‌های 4.0.0 تا 4.4.2
- Joomla! CMS نسخه‌های 5.0.0 تا 5.0.2

توصیه‌های امنیتی

این آسیب‌پذیری‌ها تأثیر مستقیمی بر روی سیستم‌هایی که از Joomla استفاده می‌کنند، دارند. برای جلوگیری از سوءاستفاده‌های احتمالی، پیشنهاد می‌شود که کاربران به سرعت به آخرین نسخه‌های امنیتی بروزرسانی کنند.

1- MFA

آسیب‌پذیری در افزونه Plugin Groups وردپرس

یک آسیب‌پذیری با شناسه CVE-2024-1108 و شدت 6.5 در افزونه Plugin Groups وردپرس شناسایی شده است. این آسیب‌پذیری به دلیل عدم وجود بررسی مجوز در تابع admin_init() در افزونه Plugin Groups رخ می‌دهد. این نقص به مهاجمان غیرمجاز اجازه می‌دهد تا تنظیمات افزونه را تغییر دهند، این امر می‌تواند موارد زیر را به دنبال داشته باشد:

- دستکاری داده‌ها: مهاجم می‌تواند تنظیمات افزونه را برای تغییر رفتار آن تغییر دهد.
- عدم سرویس[1]: مهاجم می‌تواند تنظیمات افزونه را به گونه‌ای تغییر دهد که موجب خرابی یا ناپایداری وب‌سایت شود.

محصولات تحت تاثیر

تمام نسخه‌های این افزونه از نسخه 2.0.0 تا نسخه 2.0.6 در معرض این آسیب‌پذیری قرار دارند.

توصیه‌های امنیتی

توصیه می‌شود که افزونه Plugin Groups به آخرین نسخه یعنی 2.0.9 به‌روزرسانی شود.

1- DoS

مجرم سایبری

گرگ در لباس گوسفند

بدترین اقدامات، هوشمندانه انجام می‌شوند.


مرکز آپا دانشگاه سمنان
آموزش
امنیت
سایبری

آشنایی با پروتکل CDP و بررسی نمونه‌ای از این پروتکل در وایرشارک

پروتکل CDP چیست؟

پروتکل CDP[1] یک پروتکل لایه دو[2] است که در سال 1994 توسط سیسکو[3] ارائه شده است. هدف این پروتکل به اشتراک گذاشتن اطلاعات دیوایس‌های سیسکویی است که بطور مستقیم متصل هستند. این اطلاعات می‌تواند شامل نسخه سیستم عامل، آدرس IP و ... باشد.

دیوایس‌های سیسکو بسته‌های CDP را با مک آدرس مقصد[4] 01:00:0c:cc:cc:cc از هر اینترفیس[5] متصلی خارج می‌کنند. این فریم‌ها[6] از سوییچ‌های سیسکو و یا هر دستگاه شبکه‌ای که متصل است Multicast می‌شوند. این نوع Multicast کردن در پروتکل‌های دیگر سیسکو مانند پروتکل ترانکینگ[7] در VLAN[8] هم استفاده می‌شود. بطور پیش فرض CDP هر 60 ثانیه بر روی اینترفیس‌هایی که از پروتکل SNAP[9] پشتیبانی می‌کنند (مانند اترنت، Frame Ralay[10] و ATM[11]) ارسال می‌شوند. هر دستگاه سیسکو که از CDP پشتیبانی می‌کند، اطلاعات دریافتی از دستگاه‌های دیگر را در یک جدول ذخیره می کند که با استفاده از دستور show cdp همسایگان قابل مشاهده است. این جدول همچنین از طریق پروتکل SNMP[12] قابل دسترسی است. اطلاعات جدول CDP پس از دریافت هر اعلانی به روز شده و زمان holdtime آن از ابتدا شروع می‌شود. holdtime مدت زمان ماندگاری هر ورودی جدول را مشخص می‌کند که بطور پیش فرض 180 ثانیه است اگر در این مدت هیچ اعلان جدیدی نرسد دستگاه تمام اطلاعات جدول را دور می‌ریزد.

1- Cisco Discovery Protocol
2- Data Link
3- Cisco
4- Destination MAC Address
5- Interface
6- Frame
7- Trunking
8- Virtual Local Area Network
9- Subnetwork Access Protocol
10- یک فناوری استاندارد برای شبکه WAN
11- Asynchronous Transfer Mode
12- Simple Network Management Protocol

پروتکل CDP چه اطلاعاتی را رد و بدل می‌کند؟

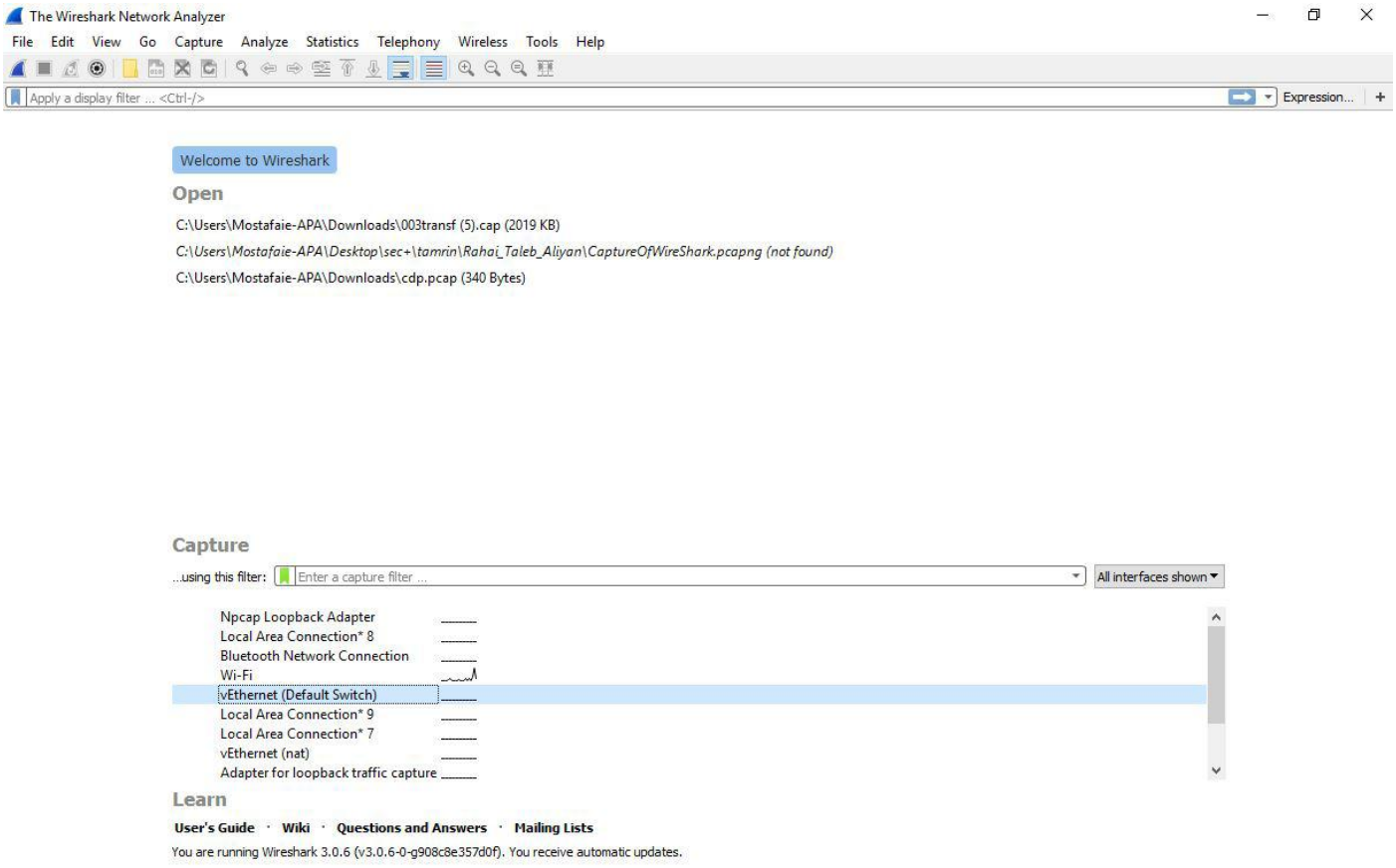
اطلاعـات موجـود در CDP بـا توجـه بـه نـوع دسـتگاه و نسـخه سیسـتم عامـل موجـود در آن متفـاوت اسـت. ایـن اطلاعـات ممکـن اسـت شـامل نسـخه سیسـتم عامـل، نـام میزبـان[1]، آدرس IP از کلیـه پروتـکل (هـای) تنظیـم شـده در پـورت کـه در آن فریم CDP ارسـال شـده اسـت، شناسـه پـورت کـه از آن CDP ارسـال شـده اسـت، نـوع دسـتگاه و مـدل، تنظیمـات Duplex ، دامنـه native VLAN، VTP ، کشـش بـرق (بـرای تـوان دسـتگاه‌های اترنـت) و سـایر اطلاعـات خـاص دسـتگاه باشـد. جزئیـان ایـن اطلاعیه‌هـا بـه دلیـل اسـتفاده از قالـب TLV (type-length-value) می‌توانـد گسـترش یابـد.

پروتکل CDP در دونسخه‌ی 1 و 2 موجود است که به طور پیش فرض نسخه‌ی 2 در همه‌ی دستگاه‌ها فعال است.

مشاهده جزئیات پروتکل CDP در وایرشارک

کابل LAN را از سیستمی که وایرشارک روی آن نصب است به یک پورت که به دیوایس سیسکو متصل است میزنیم.

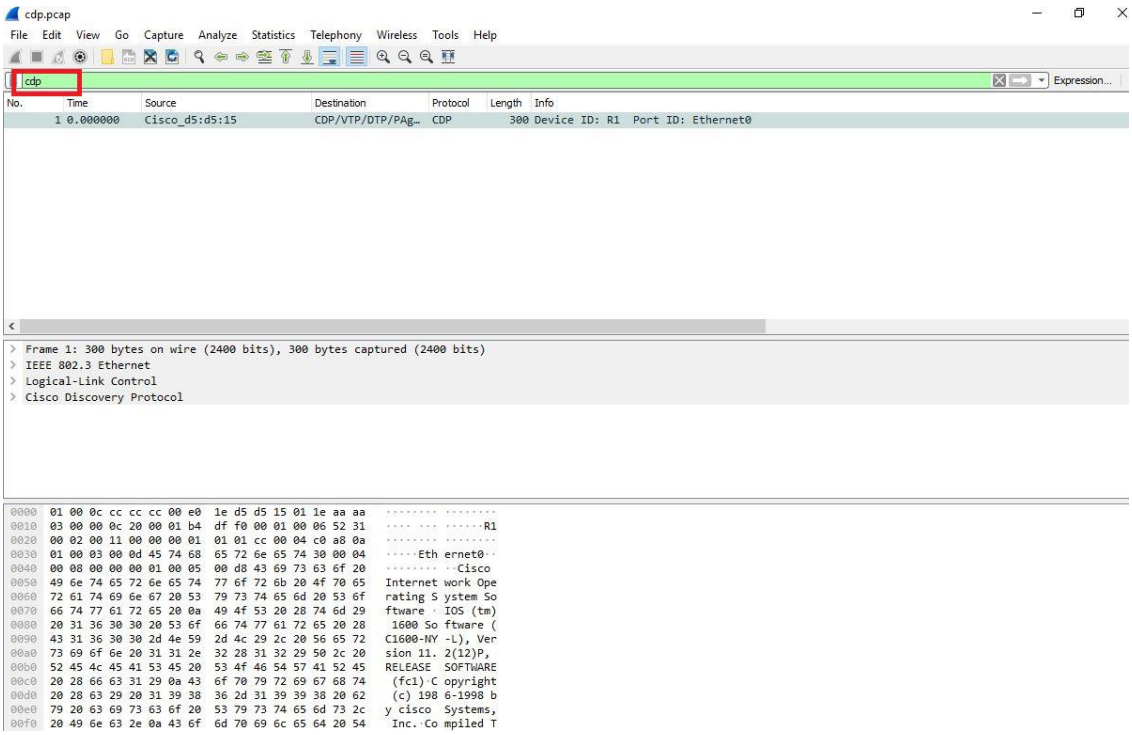
وارد نرم افزار وایرشارک میشویم و روی پورت اترنت شروع به Capture گرفتن می‌کنیم.



شکل ۱: نمایی از صفحه‌ی ورودی نرم افزار وایرشارک

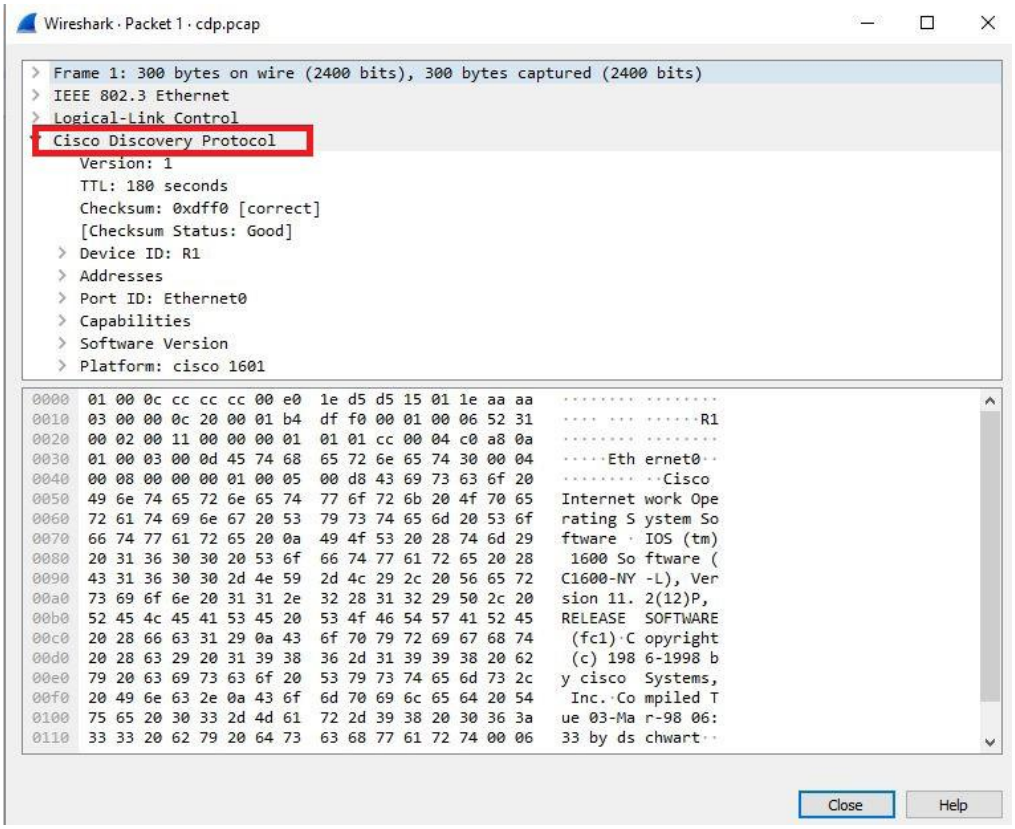
حال در بسته‌های Capture شده با فیلتر کردن "cdp" به دنبال فریم پروتکل CDP می‌گردیم.

1- hostname



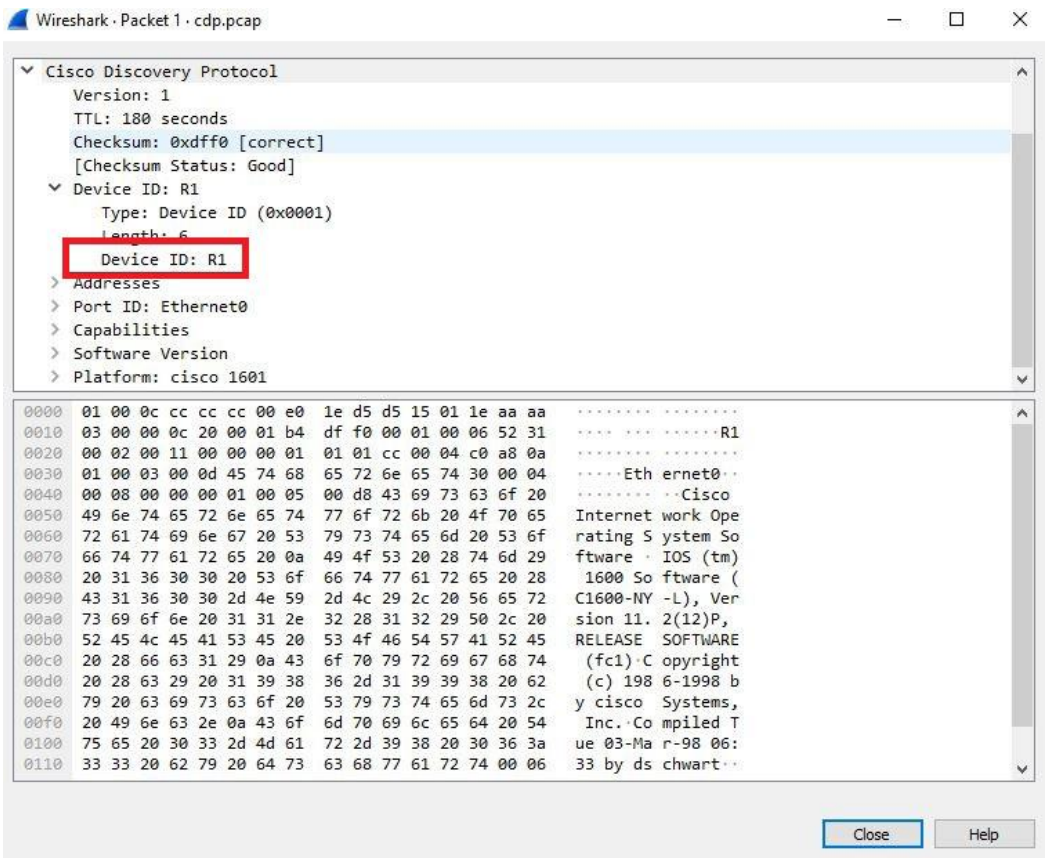
شکل۲: نحوه فیلتر کردن برای دستیابی به فریم CDP

با دابل کلیک کردن روی فریم CDP پنجره جدیدی باز می‌شود که در آن به اطلاعات CDP دسترسی خواهیم داشت.



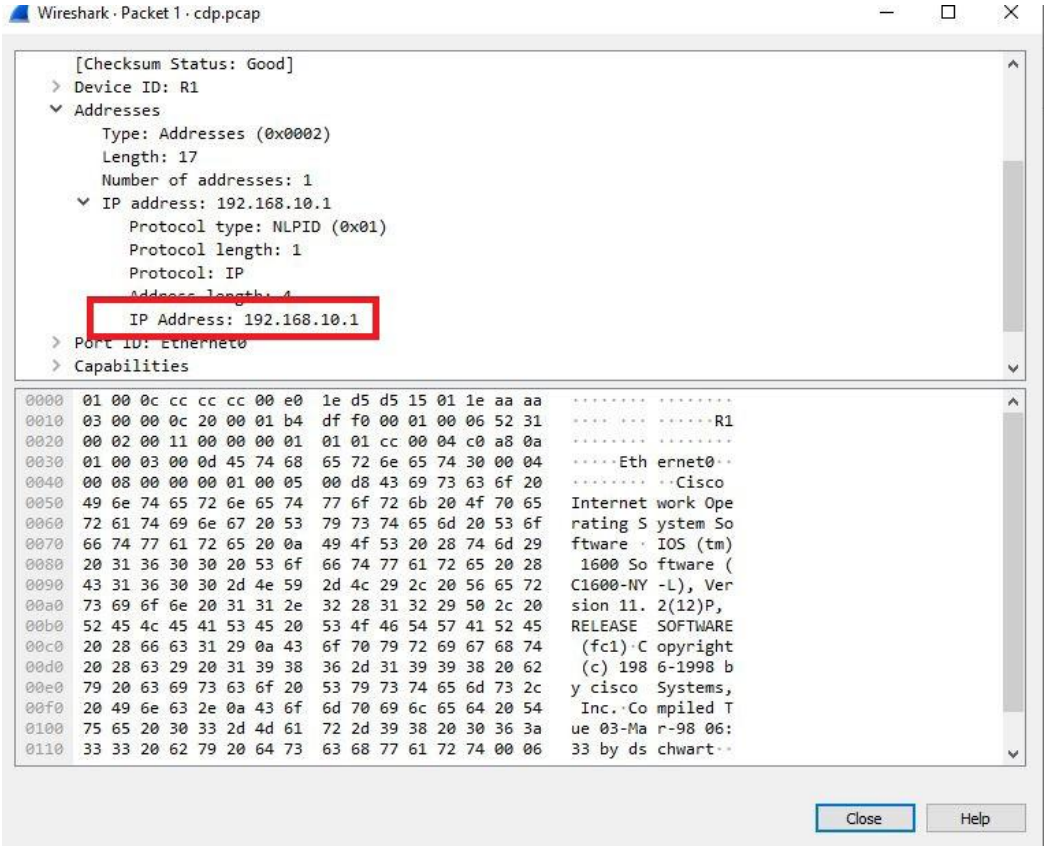
شکل۳: دستیابی به اطلاعات پروتکل CDP

همانطور که در تصویر بالا مشخص است دستگاهی که پروتکل CDP از آن خارج شده است از CDP v1 استفاده کرده است. گزینه بعدی Device ID است. همانطور که در تصویر زیر می‌بینید دستگاهی که به آن متصل شده‌ایم R1 نام دارد.



شکل ۴: پیدا کردن ID دستگاه از طریق پروتکل CDP

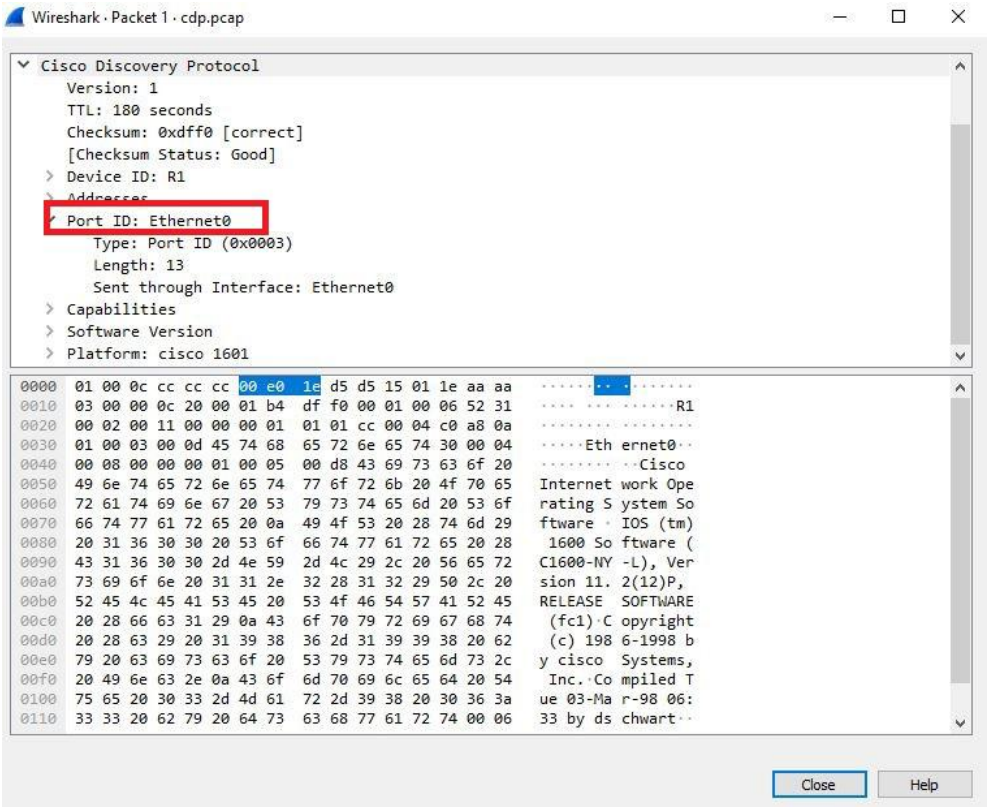
برای پیدا کردن IPدستگاه وارد بخش Addresses می‌شویم.



شکل ۵: پیدا کردن IP دستگاه با استفاده از پروتکل CDP

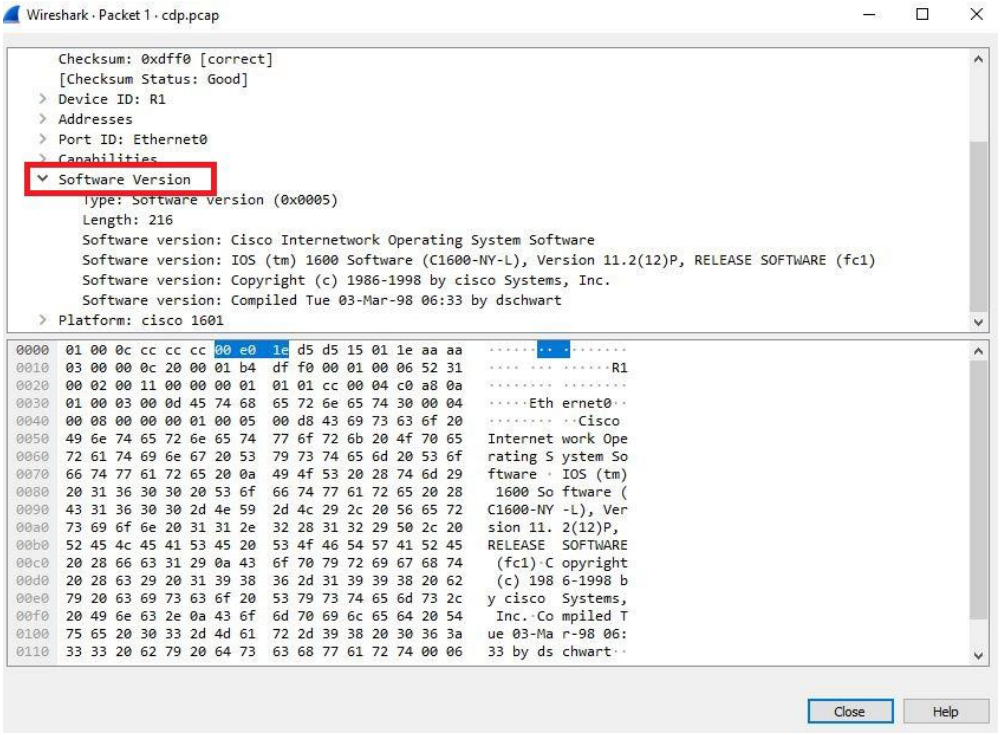
همانطور که مشخص است IP دستگاهی که به آن متصل هستیم 192.168.10.1 می‌باشد.

برای اینکه بدانیم به کدام پورت بطور مستقیم متصل هستیم از طریق منوی Port ID اقدام میکنیم. مشاهده می‌شود که به پورت Ethernet0 متصل شده‌ایم.

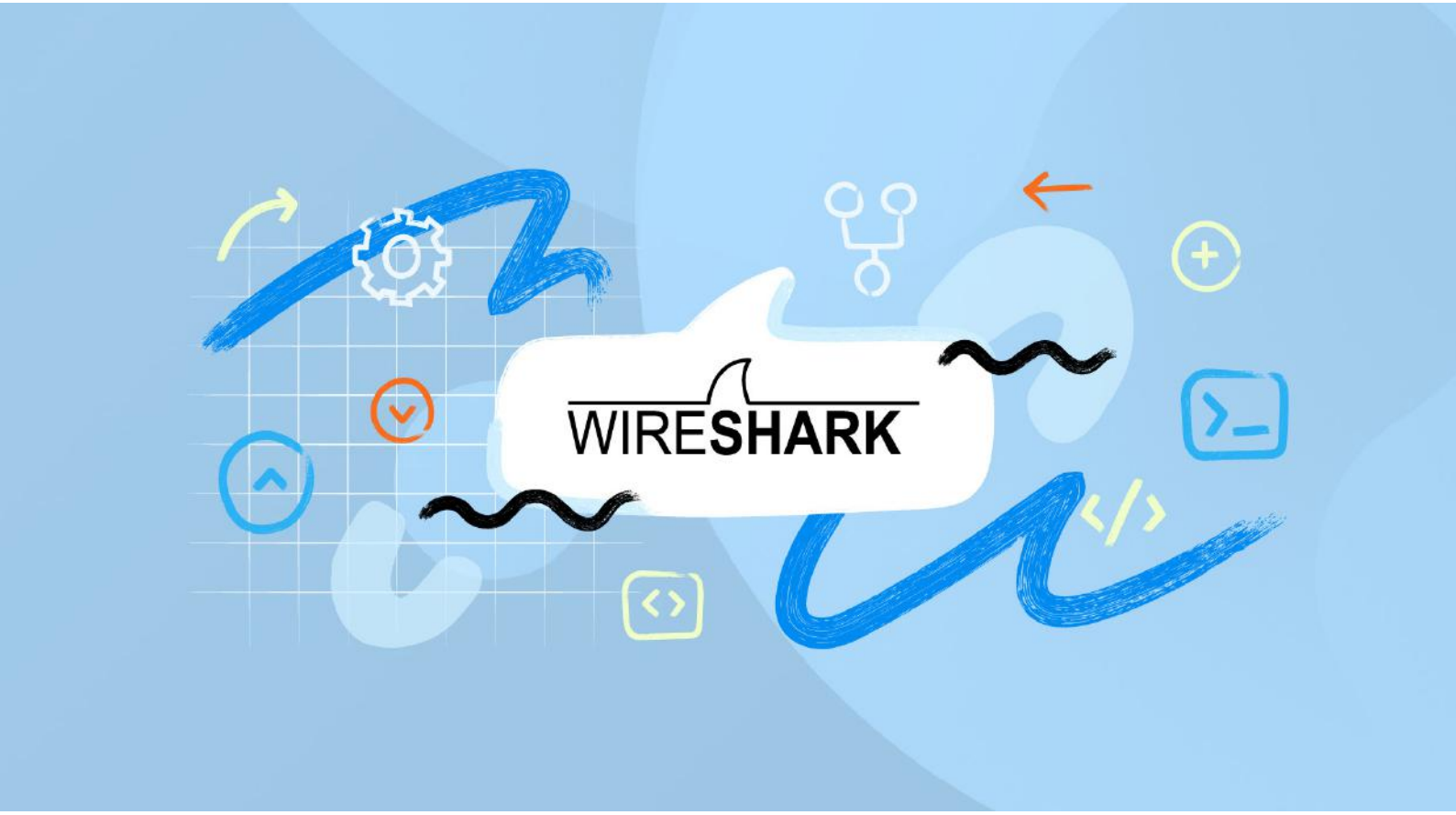


شکل۶: پیدا کردن پورت از روی پروتکل CDP

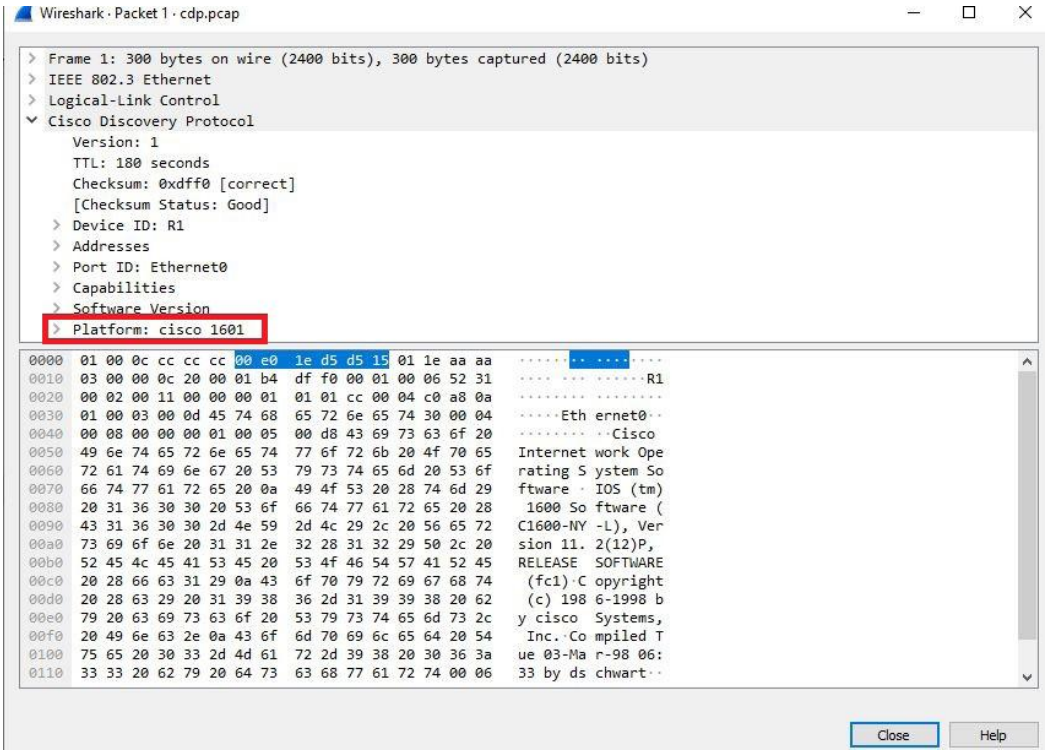
برای یافتن نوع سیستم‌عاملی در حال اجرا و نسخه‌ی آن از بخش Software Version استفاده خواهیم کرد.



شکل۷: پیدا کردن سیستم عامل از روی پروتکل CDP



بـرای یافتـن نـوع دسـتگاه از بخـش Platform اسـتفاده می‌کنیـم. همانطـور کـه مشـاهده می‌شـود مـا در ایـن سـناریو بـه یـک سـوییچ سیسـکو ۱۶۰۱ متصـل هسـتیم.



شکل ۸: پیدا کردن پلتفرم از روی پروتکل CDP

تلاش ما
حفظ امنیت
شماست...