مرکز آپا دانشگاه سمنان

خبرنامه الکترونیکی ۷۲

مرکز تخصصی آپا دانشگاه سمنان

در این شماره می‌خوانید:

شماره هفتاد و دو ، سال هشتم، دی ۱۴۰۴ |کاری از تیم تولید محتوای مرکز تخصصی آپای دانشگاه سمنان

https://cert.semnan.ac.ir info.cert@semnan.ac.ir ۰۲۳-۳۱۵۳۵۰۲۱ @semcert

فهرست

خبر

آموزش

مرکز آپا دانشگاه سمنان

اخبار امنیت سایبری

کشف آسیب‌پذیری در کتابخانه SNMP

net-snmp یک کتابخانه برنامه‌های کاربردی SNMP به‌همراه مجموعه‌ای از ابزارها و یک دیمون (daemon) است. در نسخه‌های قبل از ۵.۹.۵ و pre۲.۵.۱۰، ارسال یک بسته خاص و دست‌کاری‌شده به دیمون snmptrapd در net-snmp می‌تواند باعث سرریز بافر شده و موجب از کار افتادن دیمون شود.

محصولات تحت تاثیر:

نسخه‌های قبل از ۵.۹.۵ و pre۲.۵.۱۰

توصیه های امنیتی:

تبه کاربران توصیه میشود در صورت استفاده از این کتابخانه پورت‌های SNMP را به روی شبکه‌های عمومی ببندند. اطمینان حاصل شود که پورت‌های مربوط به snmptrapd به‌درستی توسط فایروال محافظت شده‌اند. همچنین به کاربران توصیه میشود آن را به نسخه ۵.۹.۵ و pre۲.۵.۱۰ به روزرسانی نمایند.

کشف آسیب‌پذیری در پیاده‌سازی ONVIF دوربین‌های IP Xiongmai XM۵۳۰

آسیب‌پذیری CVE-۲۰۲۵-۶۵۸۵۶ با شدت ۹.۸ یک نقص امنیتی جدی در دوربین‌های تحت شبکه Xiongmai XM۵۳۰ است که از پیاده‌سازی نادرست پروتکل ONVIF ناشی می‌شود. در این وضعیت، مکانیزم احراز هویت برای ده‌ها endpoint حساس به درستی اعمال نشده و مهاجم می‌تواند بدون نیاز به نام کاربری یا رمز عبور به آن‌ها دسترسی پیدا کند. این نقص به مهاجمان راه دور اجازه می‌دهد اطلاعات حساس دستگاه، تنظیمات سیستمی و حتی جریان زنده ویدئو را مشاهده کنند. نبود کنترل دسترسی روی این endpointها باعث نقض کامل محرمانگی کاربران می‌شود. در محیط‌های سازمانی یا نظارتی، این موضوع می‌تواند پیامدهای جدی امنیتی و حریم خصوصی به همراه داشته باشد. سادگی بهره‌برداری، این آسیب‌پذیری را به تهدیدی پرخطر برای کاربران این دوربین‌ها تبدیل می‌کند.

محصولات تحت تاثیر:

دوربین‌های تحت شبکه Xiongmai مدل XM۵۳۰

نسخه آسیب‌پذیر ۲۱.۰۶ Firmware: V۵.۰۰.R۰۲.۰۰۰۸۰VD۸.۱۰۰۱۰.۳۴۶۶۲۴.S.ONVIF

پیاده‌سازی ONVIF در این نسخه دارای نقص احراز هویت است.

توصیه های امنیتی:

به‌روزرسانی فوری Firmware دوربین‌ها به نسخه‌ای که این آسیب‌پذیری را رفع کرده است (در صورت انتشار Patch رسمی).

در صورت عدم انتشار patch، محدود کردن دسترسی شبکه‌ای به دوربین‌ها (قرار دادن آن‌ها پشت فایروال/VPN).

غیرفعال کردن ONVIF در تنظیمات دوربین اگر در حال استفاده نیست.

افزودن احراز هویت قوی (Credential و رمز عبور پیچیده) برای دسترسی به رابط مدیریتی دوربین.

استفاده از شناسایی و مسدودسازی ترافیک غیرمجاز ONVIF با WAF یا IDS/IPS شبکه.

مانیتورینگ لاگ‌ها برای شناسایی تلاش‌های غیرمجاز برای دسترسی ویدئو/اطلاعات.

جداسازی شبکه دوربین‌ها در VLAN یا شبکه‌ی مجزا برای کاهش برد حمله به بخش‌های حساس شبکه.

کشف آسیب‌پذیری در افزونه Print Invoice & Delivery Notes برای WooCommerce

آسیب‌پذیری CVE-۲۰۲۵-۱۳۷۷۳ با شدت ۹.۸ یک نقص امنیتی بحرانی در افزونه Print Invoice & Delivery Notes for WooCommerce وردپرس است که تا نسخه ۵.۸.۰ وجود دارد. این مشکل به دلیل نبود بررسی سطح دسترسی در تابع WooCommerce_Delivery_Notes::update ایجاد شده و باعث می‌شود کاربران غیرمجاز بتوانند به این تابع دسترسی پیدا کنند. در کنار این ضعف، فعال بودن اجرای کد PHP در کتابخانه Dompdf و نبود escaping مناسب در فایل template.php شرایط را برای اجرای کد دلخواه روی سرور فراهم می‌کند. مهاجم بدون نیاز به احراز هویت می‌تواند کد مخرب خود را اجرا کرده و کنترل سرور را به دست بگیرد. این آسیب‌پذیری می‌تواند منجر به سرقت اطلاعات، دستکاری سایت یا نصب بدافزار شود. به دلیل سادگی بهره‌برداری و تأثیر گسترده، این نقص یک تهدید جدی برای وب‌سایت‌های ووکامرسی محسوب می‌شود.

محصولات تحت‌تأثیر:

افزونه: Print Invoice & Delivery Notes for WooCommerce

پلتفرم: وب‌سایت‌های WordPress که از ووکامرس استفاده می‌کنند

نسخه‌های آسیب‌پذیر: تمام نسخه‌ها تا و شامل ۵.۸.۰.

توصیه های امنیتی:

به‌روزرسانی فوری افزونه به آخرین نسخه‌ی وصله‌شده (جدای از نسخه‌های ≥ ۵.۸.۰).

حذف/غیرفعال‌سازی موقت افزونه در صورت عدم نیاز تا زمان رفع کامل.

فعال‌سازی فایروال وب (WAF) برای جلوگیری از درخواست‌های مخرب به تابع update.

بررسی لاگ‌ها برای شناسایی تلاش‌های غیرمجاز برای اجرای کد.

محدود کردن دسترسی به بخش‌های مدیریتی و APIهای مرتبط با این افزونه.

استفاده از پلاگین‌های امنیتی وردپرس مانند Wordfence یا iThemes Security.

مانیتورینگ مداوم فایل‌ها و دایرکتوری‌های حساس برای شناسایی تغییرات ناخواسته.

مرکز آپا دانشگاه سمنان

آموزش امنیت سایبری

آموزش کامل بررسی پکت های گوشی اندروید با Tcpdump

مقدمه

در تحلیل شبکه، امنیت، دیباگ اپلیکیشن‌ها و بررسی رفتار ترافیکی سیستم‌عامل، دسترسی به پکت‌های خام (Raw Packets) اهمیت زیادی دارد.

در سیستم‌عامل اندروید، به‌صورت پیش‌فرض امکان مشاهده مستقیم پکت‌ها وجود ندارد؛ اما اگر گوشی Root شده باشد، می‌توان با ابزار قدرتمند Tcpdump تمام ترافیک شبکه گوشی را Capture و سپس با Wireshark تحلیل کرد.

در این آموزش یاد می‌گیریم:

- Tcpdump چیست و چه کاری انجام می‌دهد؟
- چگونه آن را روی گوشی اندروید روت‌شده نصب کنیم؟
- چطور پکت‌ها را Capture کنیم؟
- چگونه فایل‌ها را برای تحلیل به Wireshark منتقل کنیم؟
- محدودیت‌ها و نکات مهم امنیتی

Tcpdump چیست؟

tcpdump یک ابزار Command-line برای Capture و نمایش پکت‌های شبکه است که:

- در سطح Kernel کار می‌کند
- پکت‌ها را قبل از پردازش اپلیکیشن‌ها می‌بیند
- خروجی را در قالب استاندارد pcap ذخیره می‌کند

Wireshark دقیقاً همین فرمت را برای تحلیل استفاده می‌کند.

پیش‌نیازها

قبل از شروع، موارد زیر باید آماده باشد:

سخت‌افزار و نرم‌افزار

- گوشی Android روت‌شده
- کامپیوتر (Linux / Windows / macOS)
- کابل USB
- نصب بودن:

(ADB)Android Debug Bridge

Wireshark

بررسی روت بودن گوشی روی کامپیوتر:

adb shell

su

اگر پرامپت از $ به # تغییر کرد، یعنی دسترسی روت فعال است

آموزش کامل بررسی پکت های گوشی اندروید با Tcpdump

مرحله ۱: دریافت Tcpdump مناسب اندروید

نسخه‌های tcpdump باید متناسب با معماری CPU گوشی باشند.

معماری گوشی را با کامند های زیربررسی کنید :

adb shell getprop ro.product.cpu.abi

خروجی‌های رایج:

- armeabi-v۷a
- arm۶۴-v۸a
- x۸۶

دانلود tcpdump از منبع معتبر:

https://www.androidtcpdump.com

مرحله ۲: انتقال و نصب Tcpdump روی گوشی

با کامند های زیر فایل دانلودشده را به گوشی منتقل کنید:

/adb push tcpdump /sdcard

سپس:

adb shell

su

/cp /sdcard/tcpdump /system/bin

chmod ۷۵۵ /system/bin/tcpdump

بررسی نصب:

tcpdump --version

مرحله ۳: شناسایی Interface شبکه

برای Capture باید اینترفیس شبکه را بشناسیم.

ip addr

اینترفیس‌های رایج:

- wlan۰ <- اینترنت Wi-Fi
- rmnet_data۰ <- اینترنت سیم‌کارت (Mobile Data)
- lo <- Loopback (معمولاً کاربردی نیست)

مرحله ۴: شروع Capture پکت‌ها

Capture کامل ترافیک Wi-Fi:

tcpdump -i wlan۰ -w /sdcard/capture.pcap

Capture فقط HTTP و HTTPS:

tcpdump -i wlan۰ port ۸۰ or port ۴۴۳ -w /sdcard/capture.pcap

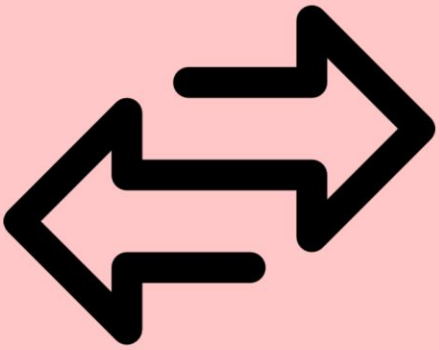
Capture ترافیک سیم‌کارت:

tcpdump -i rmnet_data۰ -w /sdcard/mobile.pcap

برای توقف Capture:

Ctrl + C

Tcpdump فقط از لحظه اجرا به بعد پکت‌ها را ذخیره می‌کند.



مرحله ۵: انتقال فایل pcap به کامپیوتر

بعد از پایان Capture:

adb pull /sdcard/capture.pcap

فایل حالا آماده‌ی تحلیل است.

مرحله ۶: تحلیل فایل در Wireshark

۱. Wireshark را باز کن

۲. فایل .pcap را Open کن

۳. از فیلترها زیر استفاده کن:

فیلترهای کاربردی:

dns

http

tls

ip.addr == ۸.۸.۸.۸

tcp.port == ۴۴۳

چه چیزهایی را می‌توان دید؟

- DNS Query و Domainها
- IP مقصد و مبدا
- TLS Handshake
- حجم، زمان و الگوی ترافیک

Capture زنده (Live Capture)

می‌توان بدون ذخیره فایل، مستقیم در Wireshark Capture گرفت:

- adb shell su -c "tcpdump -i wlan۰ -w -" | wireshark -k -i

این روش برای تحلیل لحظه‌ای بسیار کاربردی است.

محدودیت‌های مهم

- محتوای HTTPS رمزگذاری شده است
- پسوردها و دیتای حساس دیده نمی‌شوند
- دیدن Payload نیازمند:
  - MITM Proxy
  - یا استخراج TLS Keys (پیشرفته)

شایان ذکر است که Tcpdump هیچ پکت قبلی‌ای را بازیابی نمی‌کند.

نکات امنیتی و قانونی

- Capture فقط روی گوشی خودت یا با اجازه رسمی مجاز است
- شنود بدون اجازه غیرقانونی است
- این آموزش برای تنها برای یادگیری، تحلیل شبکه و تست امنیت تهیه شده است