بسمه تعالی

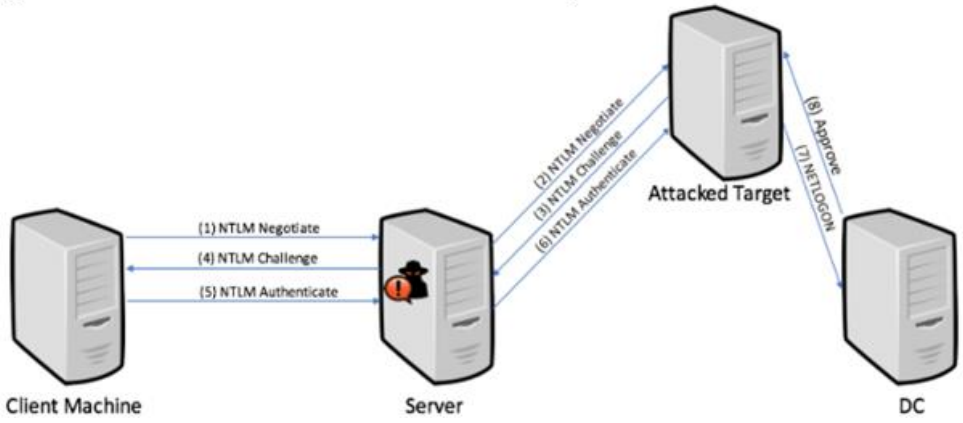
کشف باگ جدید (zero day) در پروتکل **NTLM** ویندوز

این ماه مایکروسافت یک وصله‌ی امنیتی، برای یک آسیب‌پذیری جدی (ارتقاء دسترسی) منتشر نموده است که تمامی نسخه‌های ویندوز، از ۲۰۰۷ به بعد را تحت تأثیر قرار می‌دهد.

محققان امنیتی شرکت Preempt دو آسیب‌پذیری zero-day در پروتکل امنیتی NTLM ویندوز کشف کرده‌اند، هر دوی این آسیب‌پذیری‌ها به مهاجم اجازه می‌دهند که یک دامنه جدید ایجاد نموده و آن را به طور کامل کنترل نماید.

NT LAN Manager (NTLM) یک پروتکل احراز هویت قدیمی است که در شبکه‌های شامل سیستم عامل‌های ویندوز و همچنین در سیستم‌های مستقل مورد استفاده قرار می‌گیرد.

اگرچه NTLM توسط Kerberos در ویندوز 2000 جایگزین شده است که امنیت بیشتری را در سیستم‌های شبکه‌ای فراهم آورد، اما همچنان توسط مایکروسافت پشتیبانی می‌شود و کماکان به صورت گسترده مورد استفاده قرار می‌گیرد.



در

شکل ۱ نقص NTLM

NTLM، به سادگی، هر زمان که یک کاربر می‌خواهد به سرور متصل شود، سرور یک challenge را مطرح می‌کند و کاربر challenge را با پسورد هش خود رمزگذاری می‌کند. مهاجم می‌تواند یک نشست همزمان با سروری که می‌خواهد به آن حمله کند ایجاد نماید و از همان Challenge استفاده کند، و همان هش رمزگذاری شده را به منظور ایجاد یک احراز هویت موفق در NTLM ارسال نماید. با استفاده از احراز هویتِ موفقیت‌آمیزِ NTLM، مهاجم می‌تواند یک نشست Server Message Block (SMB) را باز نموده و سیستم هدف را با نرم‌افزارهای مخرب آلوده کند.

اولین آسیب‌پذیری، Lightweight Directory Access Protocol (LDAP) حفاظت نشده از NTLM را درگیر می‌کند، و دومی Remote Desktop Protocol (RDP) را تحت تأثیر قرار می‌دهد.

LDAP به اندازه کافی در مقابل حملات NTLM مقاوم نیست، حتی زمانی که LDAP ساخته شده و معیارهای دفاعی برای آن مشخص گردیده است تنها از حملات Man-in-the-middle (MitM) محافظت می‌کند، نه از رد و بدل شدن اعتبارسنجی‌ها.

این آسیب‌پذیری به مهاجم با دسترسی SYSTEM بر روی سیستم هدف، اجازه می‌دهد که از نشست‌های NTLM ورودی استفاده نموده و عملیات LDAP را انجام دهد، مانند به روزرسانی objectهای دامنه از طرف کاربر NTLM.

Yaron Zinar از Preempt در رابطه با جزئیات آسیب‌پذیری می‌گوید: "به منظور پی بردن به میزان حساسیت موضوع، باید تمامی پروتکل‌های ویندوز، که از API احرازِ هویتِ ویندوز (SSPI) استفاده می‌کنند و اجازه می‌دهند نشست احراز هویت به سمت NTLM سوق یابد را بررسی نمود."

" درنتیجه، هر اتصالی در سیستم‌های مورد استفاده نظیر (SMB, WMI, SQL, HTTP) با کاربری ادمین به مهاجم اجازه دسترسی به تمام قابلیت‌های ویندوز را می‌دهد. "

دومین آسیب‌پذیریِ NTLM پروتکل Remote Desktop Protocol Restricted-Admin mode را تحت تأثیر قرار می‌دهد. حالتِ RDP Restricted-Admin به کاربران این امکان را می‌دهد که بدون وارد نمودن پسورد از راه دور به یک کامپیوتر متصل گردند.

به گفته‌ی محققانِ Preempt، RDP Restricted-Admin به سیستم‌های احراز هویت اجازه می‌دهد که به سمت NTLM سوق یابند. این بدان معنی است که حملات صورت گرفته با NTLM، مانند اعتبارسنجی و کرک نمودن پسورد، علیه RDP Restricted-Admin نیز می‌تواند اجرا گردد.

زمانی که با آسیب‌پذیری LDAP همراه باشد، مهاجم می‌تواند هر زمان که یک ادمین با RDP Restricted-Admin متصل می‌شود یک دامنه‌ی جعلی با حساب کاربری ادمین ایجاد نماید و کنترل کل دامنه را به دست بگیرد.

محققان در ماه آپریل آسیب‌پذیری‌های LDAP و RDP در NTLM را کشف نموده و به صورت مخفیانه به مایکروسافت گزارش نمودند. با این حال، مایکروسافت آسیب‌پذیری NTLM LDAP را در ماه مَی اعلام کرد، و نام CVE-2017-8563 را به آن اختصاص داد، اما باگ RDP را رد نمود، و ادعا کرد که این یک مسئله‌ی شناخته شده است و باید جهت مصون ماندن از هر گونه حمله‌ی NTLM شبکه را پیکربندی نمود.

مایکروسافت در مشاوره خود توضیح داد: "در سناریوی یک حمله‌ی از راه دور، مهاجم می‌تواند با اجرای یک اپلیکیشن خاص جهت ارسال ترافیک مخرب به Domain Controller این آسیب‌پذیری را اکسپلویت نماید. مهاجمی که موفق به اکسپلویت نمودن این آسیپ‌پذیری شد می‌تواند پروسه‌ها را در یک بستر بالقوه اجرا کند."

برای مصون ماندن از این آسیب‌پذیری‌ها چه کاری باید انجام داد؟

۱. نصب وصله‌ی امنیتی CVE-2017-8563 بر روی تمامی Domain Controllerها. اگر شما به روزرسانیِ نرم‌افزارِ خودکار داشته باشید، احتمالاً قبلاً تحت پوشش قرار گرفته‌اید، اما به یاد داشته باشید برای اینکه وصله‌ی امنیتی کار کند باید Domain Controller را ریستارت نمایید.
۲. فعال نمودن "Require LDAP Signing" در تنظیمات GPO (درخواست کنید بسته‌های LDAP و SMB ورودی، به صورت دیجیتالی امضا شوند). این ویژگی به صورت پیش فرض بر روی "on" تنظیم نشده است و بسیار شبیه "SMB Signing" می‌باشد، اگر تنظیمات به درستی پیکربندی نشده باشند شما در معرض خطر قرار دارید.
۳. احراز هویت LDAP را از طریق SSL/TLS امن‌تر کنید.
۴. ترافیک NTLM را بر روی شبکه‌ی خود کنترل نمایید و هرگونه استفاده غیرمعمول و ناشناخته را مجدداً مرور کنید.
۵. مجوز دسترسی دامنه‌ی خود را به کسی ندهید (در صورت لزوم، دو حساب کاربری داشته باشید، یکی برای کمک‌های از راه دور و دیگری با دسترسی‌های کاربری ادمین). برای این منظور توصیه می‌کنیم راهنمای Pass-the-Hash مایکروسافت برای تقسیم‌بندی شبکه را مطالعه نمایید.

علاوه بر نقصِ NTLM، مایکروسافت وصله‌های امنیتی را برای ۵۵ آسیب‌پذیری امنیتی منتشر نموده است، که شامل ۱۹ مورد مهم در تعدادی از محصولاتش می‌باشد، از جمله Edge، Internet Explorer، Windows، Office و Office Services و Web Apps، NET Framework، و Exchange Server .

کاربران ویندوز بسیار توصیه می‌کنند که جهت مصون ماندن از حملات فعالی که هر لحظه ممکن است اتفاق بیفتد آخرین به روز رسانی‌ها را حتماً در اسرع وقت نصب نمایید.

منبع:

http://thehackernews.com/2017/07/windows-ntlm-security-flaw.html

https://blog.preempt.com/new-ldap-rdp-relay-vulnerabilities-in-ntlm