بسمه‌تعالی

یک چالش امنیتی در تکنولوژی مدیریت فعال (AMT) شرکت اینتل

۱ مقدمه

پس از کشف حملات Meltdown و Spectre، شرکت اینتل[۱] در آشوبی سهمگین به‌سر می‌برد. محققان امنیتی، موفق به کشف یک آسیب‌پذیری جدید در تکنولوژی مدیریت فعال (AMT)[۲] شرکت اینتل شده‌اند که می‌تواند توسط مهاجمان از راه دور، اکسپلویت شود و امکان دست‌یابی به چندین لپ‌تاپ شرکتی را طی چند ثانیه فراهم آورد. در شرایط کنونی، میلیون‌ها دستگاه، به‌صورت بالقوه در معرض حملات قرار دارند.

آسیب‌پذیری موجود در سخت‌افزار اینتل، توسط متخصصان امنیتی سازمان F-Secure کشف گردید. این معضل، AMT اینتل را، که یک تکنولوژی سخت‌افزاری و سفت‌افزاری برای مدیریت خارج از باند از راه دور کامپیوترهای شخصی به‌شمار می‌رود، در راستای کنترل، نگهداری، به‌روزرسانی، ارتقا، و تعمیر آنها تحت تاثیر قرار می‌دهد. آسیب‌پذیری مذکور، در سطح تراشه انجام می‌پذیرد و به نرم‌افزار و یا سیستم‌عامل بستگی ندارد.

در جولای ۲۰۱۷ میلادی، هَری سینتونن[۳]، یکی از مشاوران امنیتی ارشد F-Secure، به رفتار ناامن و گمراه‌کننده‌ی پیش‌فرض موجود در AMT پی برد.

حمله می‌تواند اکسپلویت شود تا دسترسی کامل از راه دور به یک شبکه‌ی شرکتی را بدون در اختیار داشتن مهارت خاصی، ممکن سازد.

آسیب‌پذیری می‌تواند توسط مهاجمین و از طریق دسترسی فیزیکی به ماشین‌های تحت تاثیر، اکسپلویت شود تا احراز هویت (اطلاعات اعتباری ورودی، رمزهای عبور BIOS و BitLocker، و کدهای پین[۴] TPM) را نادیده بگیرد (دور بزند) و مدیریت از راه دور پس از استثمار را فراهم آورد.

---

[۱] Intel

[۲] Active Management Technology (AMT)

[۳] Harry Sintonen

[۴] Pin

این بدان معنا است که حتی اگر BIOS توسط یک رمزعبور حفاظت شود، امکان دست‌یابی به توسعه‌ی AMT BIOS (توسعه‌ی BIOS موتور مدیریتی (MEBx)[۵] اینتل) وجود دارد. رمزعبور پیش‌فرض "admin"، امکان دست‌یابی به AMT را برای مهاجمان فراهم می‌کند.

سناریوی حمله، این امکان را برای مهاجمان فراهم می‌آورد تا دسترسی فیزیکی به ماشین داشته‌باشند و از این طریق، دستگاه را با فشردن کلیدهای CTRL-P در طول فرایند، بوت[۶] (راه‌اندازی) نمایند و توسط "admin"، وارد MEBx شوند.

فرایند نصب، آسان است: یک مهاجم، حمله را با راه‌اندازی مجدد ماشین هدف (قربانی) و پس از آن‌که منوی بوت را وارد می‌کند، آغاز می‌نماید. در شرایط عادی، یک نفوذگر باید در این نقطه متوقف شود، زیرا از رمزعبور BIOS مطلع نیست و نمی‌تواند هیچ آسیبی به کامپیوتر وارد نماید.

اگرچه، در این حالت، مهاجم یک راه‌حل نزد خود دارد: AMT! وی می‌تواند با انتخاب MEBx و با بهره‌گیری از رمزعبور پیش‌فرض "admin"، وارد سیستم شود؛ زیرا غالبا، کاربران مبادرت به تغییر این رمزعبور نمی‌نمایند. یک مجرم سایبری سریع، به‌طور موثر، با تغییر رمزعبور پیش‌فرض، فعال نمودن دسترسی از راه دور، و تنظیم opt-in کاربر AMT به "None"، ماشین را به اختیار خود درمی‌آورد.

هنگامی‌که دسترسی از راه دور فعال می‌شود، مهاجم قادر خواهدبود از راه دور به سیستم دست یابد و بخش‌های همان شبکه را با قربانی به اشتراک بگذارد.

شاید با خود بگویید که اکسپلویت کردن به قرابت فیزیکی نیاز دارد، اما محققان F-Secure اذعان دارند که این امر، برای مهاجمان خبره‌ای که حمله‌ی Evil Maid را قدرت بخشیده‌اند، کار پیچیده و دشواری نیست.

مهاجمان، هدفی را که قصد دارند اکسپلویت نمایند، شناسایی و مکان آن را مشخص می‌کنند. آنها، در یک مکان عمومی-فرودگاه، کافه، و یا لابی هتل- به هدف نزدیک می‌شوند و سناریوی Evil Maid را به‌کار می‌بندند. لزوما، یک مهاجم، علامت را منحرف می‌کند و دیگری، مختصرا به لپ‌تاپ قربانی دسترسی پیدا می‌کند. حمله، به زمان زیادی نیاز ندارد. کل عملیات می‌تواند در کمتر از یک دقیقه انجام پذیرد.

---

[۵] Management Engine BIOS Extension (MEBx)

[۶] Boot

۱.۱ تکنولوژی AMT

AMT، یک راه‌حل اختصاصی اینتل در راستای کنترل دسترسی از راه دور و نگهداری کامپیوترهای شخصی شرکتی است. هدف از ایجاد این تکنولوژی، بهبود کنترل دستگاه‌های شرکت‌ها توسط گروه‌های IT و یا تامین‌کنندگان سرویس مدیریت‌شده است. AMT به مدیریت سیستم این فرصت را می‌دهد تا وظایف دشوار مرتبط با IT در طول سیم را از طریق اتصال از راه دور به یک ماشین، هدایت کند و کنترل آن را از کاربر بگیرد. به‌دلیل آن‌که AMT از مفهوم سیستم‌عامل جدا بوده و به آن وابسته نیست، حتی وقتی‌که کامپیوتر خاموش است، در طول زمانی که به پریز برق متصل بوده و یک کابل شبکه به آن وصل شده، کار می‌کند.

AMT، در کامپیوترهایی که حاوی پردازنده‌های vPro-enabled اینتل و نیز پلتفرم‌های ایستگاه کاری مبتنی بر پردازنده‌های خاص Intel Xeon هستند، یافت می‌شود. به‌دلیل آن‌که اکثر لپ‌تاپ‌ها از تکنولوژی اینتل استفاده می‌کنند، AMT می‌تواند در طیف گسترده‌ای از نقاط انتهایی شرکت یافت شود.

۲.۱ حمله‌ی Evil Maid

یک حمله‌ی Evil Maid، یک اکسپلویت امنیتی است که یک دستگاه محاسباتی خاموش و متصل‌نشده را مورد هدف قرار می‌دهد. طی یک حمله‌ی Evil Maid، مهاجم قادر خواهدبود چندین‌بار و بدون اطلاع مالک، دسترسی فیزیکی به دستگاه داشته‌باشد.

برای درک بهتر این حمله، سناریوی زیر را درنظر بگیرید:

- **صحنه‌ی نخست**: یک مدیر ارشد مالی (CFO)[۷]، در یک کنفرانس حضور دارد. وی جهت صرف شام با همتایان خود، لپ‌تاپ خود را در اتاق هتل خود ترک می‌نماید. او مطمئن است که هر داده‌ی یکپارچه‌ی موجود روی لپ‌تاپ، در امنیت قرار دارد؛ زیرا هارددرایو وی رمزگذاری شده‌است.
- **صحنه‌ی دوم**: یک Evil Maid (که در واقع، یک جاسوس است)، CFO که اتاق خود را ترک کرده‌است، به‌عنوان هدف درنظر می‌گیرد.
- **صحنه‌ی سوم**: Evil Maid، به‌صورت دزدکی و پنهانی، وارد اتاق CFO می‌شود و لپ‌تاپ وی را از طریق یک راه‌انداز[۸] موجود روی یک فلش USB، بالا می‌آورد (بوت می‌کند).

[۷] Chief Financial Officer (CFO)

روش راه‌اندازی مذکور، در لینوکس و ویندوز، متفاوت است:

- **لینوکس**: جهت اجرای حمله‌ی Evil Maid روی لینوکس، از دستور زیر استفاده می‌شود، که /dev/sdx باید با دستگاهی که فلش USB شما را نشان می‌دهد، جایگزین شود (به‌عنوان مثال، /dev/sdb/). دقت فرمایید، انتخاب یک دستگاه اشتباه، به هارددیسک و یا سایر تجهیزات شما آسیب خواهدزد. همچنین، اطمینان حاصل نمایید که دستگاه، کل دیسک را نمایش دهد (مانند /dev/sdb/)، نه بخشی از آن را (مانند ۱dev/sdb/):

```
dd if=evilmaidusb.img of=/dev/sdX
```

- **ویندوز**: در ویندوز، باید کار را از طریق یک برنامه‌ی dd like انجام دهید. دستور، مشابه زیر است، که HarddiskX باید با دستگاهی که فلش USB شما را نشان می‌دهد، تعویض گردد:

```
dd if=evilmaidusb.img of=\\?\Device\HarddiskX\Partition* bs=1M
```

در نهایت، Evil Maid، یک کی‌لاگر را جهت ضبط کلید رمزنگاری CFO نصب کرده و مجددا، لپ‌تاپ را خاموش می‌کند.

- **صحنه‌ی چهارم**: CFO از شام بازمی‌گردد و کامپیوتر خود را روشن می‌نماید. هیچ چیز مشکوکی وجود ندارد. بنابراین، کلید رمزگذاری خود را وارد کرده و قفل درایو دیسک را باز می‌کند.
- **صحنه‌ی پنجم**: صبح روز بعد، در حالی‌که CFO به قصد صرف صبحانه اتاق خود را ترک می‌کند، Evil Maid بازمی‌گردد و کلید رمزنگاری CFO را بازمی‌یابد.

ممکن است هدف اصلی، سرقت و فروختن کلید و یا اِعمال تغییرات به نرم‌افزار لپ‌تاپ باشد. اما هدف هرچه که باشد، لپ‌تاپ دو بار، بدون این‌که زنگ هشداری به صدا درآید، توسط شخصی ناشناس لمس گردید.

[۸] Bootloader

۲ آسیب‌پذیری AMT

معضل، به مضمون AMT مربوط می‌شود. بر این اساس، یک مهاجم قادر خواهدبود تا کنترل کامل دستگاه کاربر را در کمتر از چند ثانیه، در دست گیرد. این مشکل، بر میلیون‌ها لپ‌تاپ در جهان اثر می‌گذارد.

معمولا، یک رمزعبور BIOS، از اعمال تغییرات سطح پایین در دستگاه توسط کاربر احرازهویت‌نشده، ممانعت به‌عمل می‌آورد. اگرچه، ذات این معضل به‌گونه‌ای است که حتی اگر رمزعبور BIOS نیز تنظیم شده‌باشد، مهاجم، به آن رمزعبور جهت پیکربندی AMT نیاز نخواهدداشت. به‌علاوه، به‌علت وجود پیش‌فرض‌هایی در پیکربندی BIOS و MEBx، یک مهاجم می‌تواند با دسترسی فیزیکی، ماشینی را که از رمزعبور پیش‌فرض در AMT استفاده می‌نماید، دور بزند. سپس، وی با اتصال از راه دور به همان شبکه‌ی بی‌سیم و یا سیمی کاربر، به دستگاه دسترسی پیدا می‌کند. در موارد خاص، یک مهاجم می‌تواند AMT را برنامه‌نویسی نماید تا لزوم حضور در همان بخش از شبکه را که قربانی در آن قرار دارد، از بین ببرد.

هیچ یک از معیارهای امنیتی موجود دیگر (رمزگذاری کامل دیسک، دیواره‌ی آتش (فایروال)[۹] محلی، نرم‌افزار ضد بدافزار، و یا VPN) قادر به جلوگیری از روند اکسپلویت این چالش نیستند.

۱.۲ توصیف

AMT، بدوا توسط رمزعبور "admin" پوشش داده می‌شود. اگر AMT پیکربندی نگردد، این رمزعبور پیش‌فرض، به مهاجم اجازه می‌دهد تا با دسترسی فیزیکی به سیستم، AMT را فعال و آن را پیکربندی نماید. تنظیم رمزعبور BIOS، مانع از دست‌یابی به MEBx نمی‌شود.

۲.۲ اثر

مهاجم قادر است کنترل از راه دور سیستم را، صرف‌نظر از تنظیم رمزعبور BIOS، پین TPM، BitLocker، اطلاعات اعتباری کاربر، و فایروال محلی به‌دست آورد. حمله‌ی موفق، منجر به از دست رفتن کامل محرمانگی، جامعیت، و دسترسی‌پذیری خواهدشد.

[۹] Firewall

۳.۲ جزئیات

آسیب‌پذیری‌های کشف‌شده، امکان حمله را فراهم می‌آورند. در سناریوی تست، فرض می‌شود که رمزعبور BIOS تنظیم گردیده‌است. به‌طور خلاصه، یک مهاجم، دسترسی به دستگاه متاثر را به‌دست می‌آورد (سناریوی Evil Maid). حمله، شامل فعال‌سازی AMT، به واسطه‌ی دسترسی از راه دور است. برای غالب سیستم‌ها، فرایند طی مراحل زیر انجام می‌پذیرد:

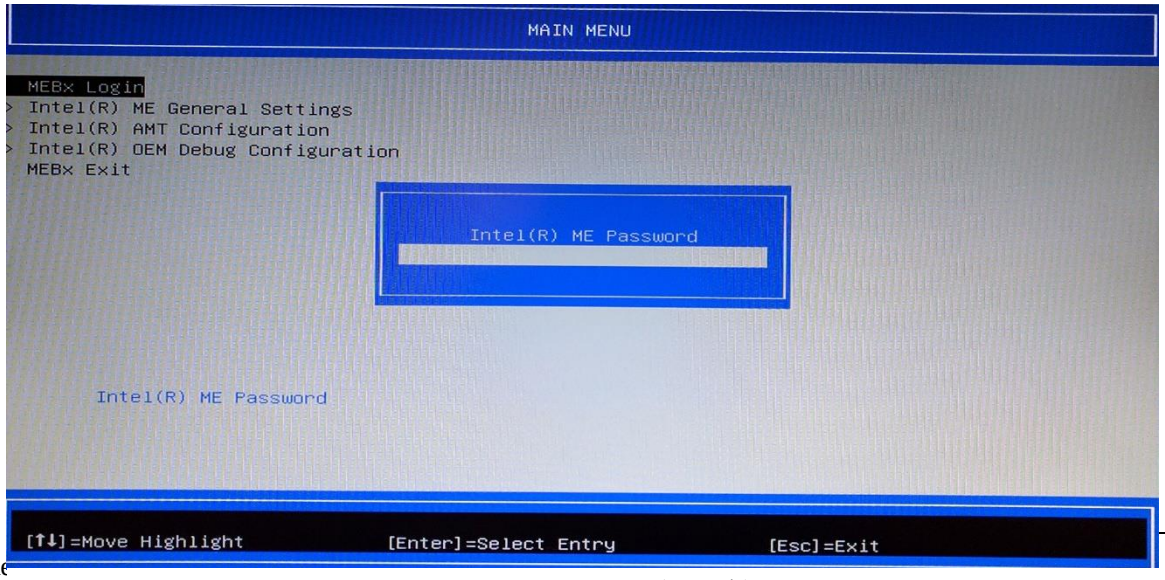
۱- سیستم را مجددا راه‌اندازی کنید[۱۰] و در طول POST، با فشردن کلیدهای CTRL-P، وارد محیط MEBx شوید.

متناوبا، در مورد لپ‌تاپ‌های Dell می‌توان به طریق زیر عمل نمود:

۱- ماشین را مجددا راه‌اندازی کنید و با فشردن کلید F۱۲ در طول POST، وارد منوی بوت شوید.
۲- MEBx را از منوی بوت انتخاب نمایید.

پس از ورود به محیط MEBx، مراحل زیر را انجام دهید:

۱- MEBx Login را انتخاب کنید.
۲- از رمزعبور "admin" استفاده نمایید.
۳- یک رمزعبور جدید را تنظیم کنید (توجه داشته‌باشید، طول این رمزعبور باید حداقل ۸ کاراکتر بوده



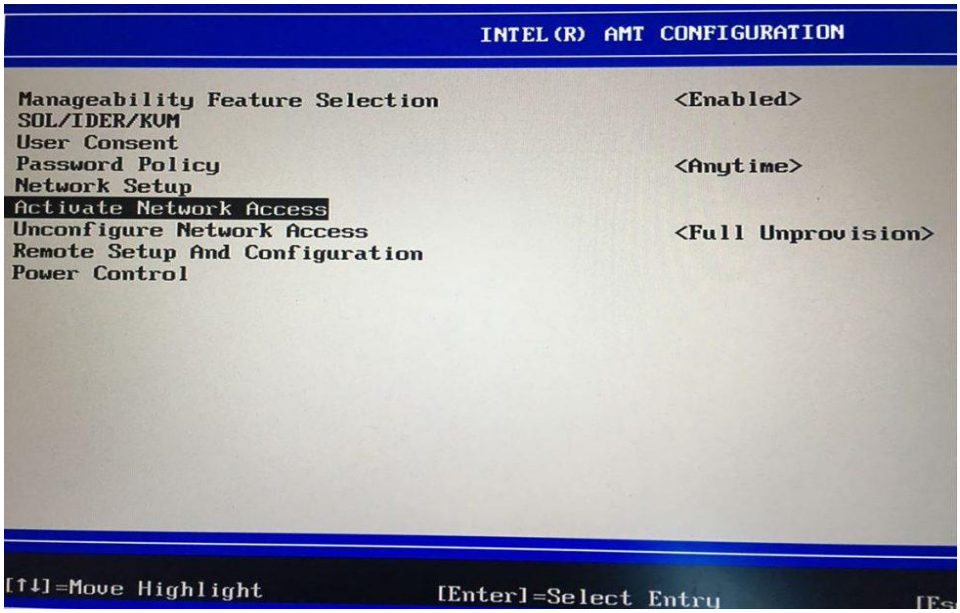
[۱۰] Re

شکل ۱: تنظیم رمزعبور جدید در MEBx

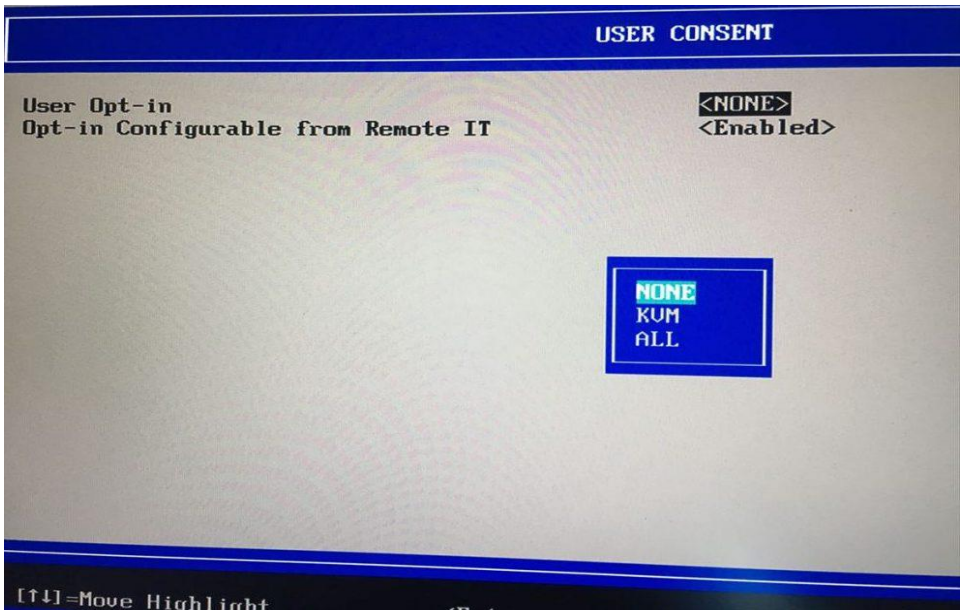
و شامل حرف بزرگ، عدد، و کاراکتر خاص باشد).

۴- Intel ® AMT Configuration را انتخاب نمایید.

۵- Active Network Access را انتخاب کرده و دسترسی از راه دور را فعال کنید.



شکل ۲: انتخاب Active Network Access

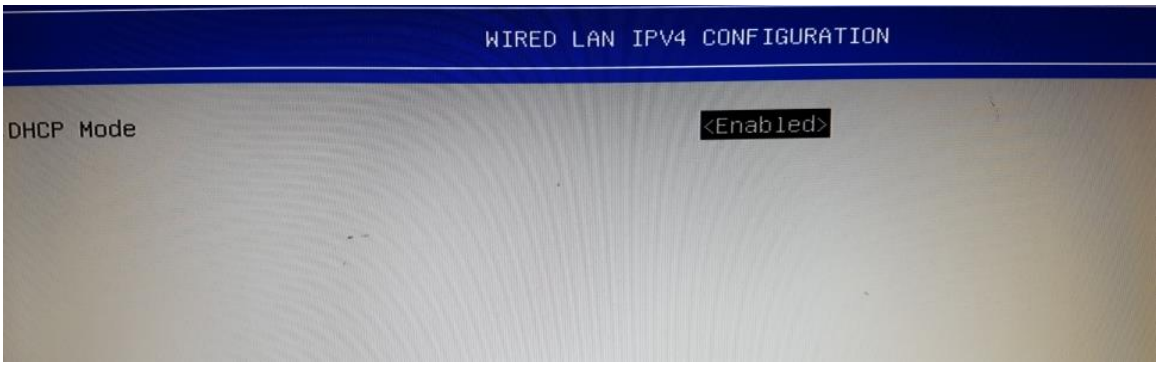


شکل ۳: تنظیم User Opt-in به NONE

۶- User Consent را انتخاب نمایید و User Opt-in را به "NONE" تغییر دهید.

۷- از منوی User Consent خارج شوید و MEBx را انتخاب کنید. با انتخاب Y، خارج خواهیدشد.

برای این‌که دسترسی از طریق Wi-Fi را ممکن سازید:



شکل ۴: فعال نمودن DHCP

۸- از طریق اترنت به سیستم وصل شوید (توجه: به سرور DHCP جهت تامین IP نیاز است).

۹- از یک مرورگر، جهت بازدید از آدرس http://TARGETIP:۱۶۹۹۲/wlan.htm استفاده نمایید (نام کاربری: admin؛ رمزعبور: رمزعبور تنظیم‌شده در گام ۳).

۱۰- Wireless Management را به Enabled in S۰, Sx/AC تغییر دهید و Submit را انتخاب کنید.

از اکنون، مهاجم قادر است از طریق شبکه‌های سیمی و بی‌سیم و با استفاده از رمزعبور تنظیم‌شده، از راه دور به سیستم دسترسی پیدا کند. جهت دسترسی به سیستم نیاز است که مهاجن، به همان بخش از شبکه دست یابد که قربانی دسترسی دارد. معمولا، دست‌یابی از طریق شبکه‌های سیمی و بی‌سیم اینتل، امکان‌پذیر است. دست‌یابی می‌تواند از طریق ابزار مختلف، مانند ابزار Open MDTK (http://www.meshcommander.com/open-manageability) انجام پذیرد.

به جای تعبیه‌ی دستی، این احتمال وجود دارد که اقدامات، توسط یک فلش USB دست‌ساز انجام پذیرد. ممکن است تامین USB، غیرفعال گردد که در این حالت، تامین دستی، تنها بردار موجود برای مهاجم خواهدبود.

به‌علاوه، این امکان وجود دارد که AMT، به‌نحوی پیکربندی گردد که مجددا، از طریق دسترسی از راه دور آغازشده توسط مشتری (CIRA)[۱۱]، به سرور مهاجم متصل گردد. در این روش، حتی در صورتی‌که مهاجم در همان بخش از شبکه نباشد، حمله کار خواهدکرد. فرض بر آن است که دستگاه هدف نمی‌تواند به اینترنت وصل شود.

در حالتی که AMT از پیش پیکربندی شده‌باشد، مهاجم می‌تواند توسط برخی دستگاه‌ها، یک تنظیم مجدد[۱۲] را برای CMOS انجام دهد. رمزعبور، به "admin" بازخواهدگشت و حمله می‌تواند همانند آن‌چه که در فوق ذکر شد، آغاز گردد.

[۱۱] Client Initiated Remote Access (CIRA)

[۱۲] Reset

۴.۲ انواع آسیب‌پذیری

۱- **کنترل دسترسی نادرست**: وقتی‌که رمزعبور ATM تنظیم نشده‌باشد، تنظیم رمزعبور BIOS نمی‌تواند مانع از دست‌یابی به MEBx گردد. پوشش داده‌نشدن توسط BIOS در این حالت، رفتاری غیرمنتظره و غافل‌گیرکننده است. در نتیجه، شماری از دستگاه‌هایی که فاقد رمزعبور AMT اینتل پیکربندی‌شده هستند، حتی در زمانی‌که تصور می‌کنند تحت پوشش رمزعبور BIOS قرار دارند، می‌توانند اکسپلویت گردند.

۲- **عدم وجود مستندسازی، منجر به پیکربندی ناامن می‌شود**: به‌دلیل عدم وجود هشدار در مورد اهمیت تغییر رمزعبور AMT، دستگاه‌های بسیاری در معرض حملات قرار می‌گیرند. پیکربندی نکردن AMT، این امکان را برای مهاجمان فیزیکی فراهم می‌آورد تا رمزعبور را پیکربندی و دسترسی از راه دور را فعال کنند.

۳- **دور زدن رمزعبور AMT**: یک مهاجم، که دسترسی فیزیکی به دستگاه دارد، می‌تواند رمزعبور را با حذف باتری CMOS، مجددا تنظیم نماید. به‌محض تنظیم مجدد، مهاجم قادر خواهدبود که AMT را از طریق MEBx فعال کرده و با استفاده از رمزعبور پیش‌فرض ذخیره‌شده (“admin”)، از راه دور دسترسی پیدا کند. در صورتی‌که سیستم مجهز به یک تراشه‌ی TPM باشد، BitLocker باید مانع از وقوع این حمله شود. به‌محض آن‌که TPM پاک می‌گردد، BitLocker می‌تواند فقط به واسطه‌ی کلید پشتیبانی، از قفل خارج شود. چنین عملی حاکی از یک بازی بی‌قاعده و مکارانه است.

۵.۲ دستگاه‌های آسیب‌پذیر

آسیب‌پذیری نوع ۱، حداقل قابل به‌کارگیری در لپ‌تاپ‌های Dell، Lenovo، Fujitsu، و HP است که از موتور مدیریت اینتل پشتیبانی می‌نمایند. به احتمال بسیار زیاد، آسیب‌پذیری مذکور بر قریب به یقین تمامی دستگاه‌هایی که AMT اینتل را پیاده‌سازی می‌کنند، اثر بگذارد. تولیدکنندگان زیر، به‌طور بالقوه، تحت تاثیر قرار دارند: Acer، Panasonic، Toshiba، Getac، Intel، و Samsung.

استثنای شایان توجهی در این زمینه وجود دارد: دستگاه‌های ASUS، آسیب‌پذیر نیستند؛ زیرا، کاربر را وادار می‌سازند تا رمزعبور BIOS را پیش از ورود به MEBx، وارد نماید.

آسیب‌پذیری نوع ۲، به مستندسازی دستگاه بستگی دارد. تاکنون، بر هیچ مستندسازی به اندازه‌ی اهمیت پیکربندی رمزعبور AMT تاکید نشده‌است.

آسیب‌پذیری نوع ۳، حداقل روی دستگاه‌های Dell، تایید شده‌است. این احتمال وجود دارد که سایر دستگاه‌ها و فروشندگان نیز در معرض این آسیب‌پذیری قرار گیرند. دستگاه‌های مبتنی بر ASUS Kaby Lake/Skylake، تحت تاثیر قرار نمی‌گیرند.

۳ توصیه‌ها

متخصصان، راه‌حل‌هایی را برای مقابله با حملات ارائه داده‌اند. جهت ممانعت از وقوع حملات Evil Maid، پیشنهاد می‌شود AMT، تنها برای دستگاه‌هایی که به آن نیاز دارند، فعال شده و برای هر دستگاه، از رمزهای عبور مبتنی بر رشته استفاده شود. فرایند تامین سیستم باید به‌روزرسانی گردد تا تنظیم یک رمزعبور قوی را برای AMT دربرگیرد، و یا حتی در صورت امکان، کاملا آن را غیرفعال نماید. اینتل نیز توصیه‌های مشابهی را در این راستا ارائه می‌دهد.

۱.۳ توصیه‌هایی به فروشندگان دستگاه

۱- در صورتی‌که رمزعبور BIOS، تنظیم شده و رمزعبور AMT هنوز تنظیم نشده‌است (AMT تامین نمی‌شود)، رمزعبور BIOS را جهت پیکربندی/تامین AMT ملزم سازید.

۲- بر اهمیت تغییر رمزعبور AMT در مستندسازی و در خود BIOS، تاکید کنید. ممکن است BIOS به‌عنوان مثال، پیامی را نشان دهد، که باید به‌صورت دستی دوره زده‌شود تا AMT، تامین و یا غیرفعال گردد. این امر، تضمین می‌نماید که پیکربندی نمی‌تواند در وضعیت ناامن باقی بماند.

۳- حذف رمزعبور AMT را دشوار سازید. حذف ساده‌ی باتری CMOS نباید این امکان را به وجود آورد تا مهاجم، کنترل دستگاه را از طریق AMT برعهده گیرد.

۲.۳ توصیه‌هایی به سازمان‌ها

۱- فرایند تامین این سیستم را به‌گونه‌ای تنظیم کنید که شامل تنظیم یک رمزعبور AMT قوی باشد. در صورتی‌که گزینه‌ی غیرفعال نمودن AMT در دسترس است، آن را انتخاب نمایید.

۲- از میان دستگاه‌های اخیرا گسترش‌یافته، گذر کرده و رمزعبور AMT را پیکربندی کنید. اگر رمزعبور، پیش از این به یک مقدار ناشناخته تنظیم شده‌است، به آن شک نموده و فرایند پاسخ تصادفی را آغاز نمایید.

۳.۳ توصیه‌ای به کاربران انتهایی

۱- با سرویس IT خود تماس بگیرید تا اوضاع را کنترل نماید. اگر شخصا دستگاه (های) خود را کنترل و اجرا می‌نمایید، حتی اگر قصد استفاده از AMT را ندارید، رمزعبور AMT خود را به یک رمز قوی تغییر دهید. اگر گزینه‌ای وجود دارد که AMT را غیرفعال می‌کند، آن را به‌کار بندید. اگر رمزعبور، از پیش به یک مقدار ناشناخته تنظیم شده‌است، به دستگاه شک کنید.

۴.۳ پاسخ اینتل

اینتل، توصیه‌هایی را به فروشندگان ارسال کرده‌است تا از MEBx اینتل، به‌واسطه‌ی رمزعبور BIOS، حفاظت کنند. همچنین، اینتل به فروشندگان توصیه کرده‌است که یک گزینه‌ی BIOS را تعبیه نمایند و از طریق آن، تامین USB را غیرفعال سازند و مقدار را به‌صورت پیش‌فرض، به غیرفعال تنظیم کنند.

۴ نتیجه‌گیری

آسیب‌پذیری مذکور، که به AMT شرکت اینتل مربوط می‌شود، از عدم توجه فروشندگان، سازمان‌ها، و کاربران انتهایی به پیکربندی رمزعبور AMT (از مقدار پیش‌فرض "admin" به یک رمزعبور قوی) نشات می‌گیرد. این آسیب‌پذیری، به نفوذگر اجازه می‌دهد تا با دسترسی فیزیکی به دستگاه هدف (طبق سناریوی Evil Maid)، تمام معیارهای امنیتی تعبیه‌شده را دور بزند، با دسترسی از راه دور به سیستم، کنترل کامل آن را در اختیار گیرد، و به KVM (صفحه‌کلید، ویدیو، و موزیک)[۱۳]، که تنظیم پیش‌فرض User Opt-in در سیستم بوت MEBx است، دست یابد. جهت ممانعت از وقوع این آسیب‌پذیری است، کافی است پیکربندی AMT را در اولویت قرار دهید و تمهیدات لازم را نیز در تنظیمات MEBx به‌کار بندید.

[۱۳] Keyboard, Video, and Music (KVM)

۵ مراجع

[۱].P. Paganini, "Security researchers from F-Secure have discovered a new issue in Intel's Advanced Management Technology (AMT) implementation that can be exploited by remote attackers to access most of the corporate laptops," Jan ۲۰۱۸, https://securityaffairs.co/wordpress/٦٧٦٧١/hacking/intel-active-management-technology-issue.html.

[۲]."Intel(R) Active Management Technology MEBx Bypass," https://sintonen.fi/advisories/intel-active-management-technology-mebx-bypass.txt.

[۳].Joel, "A Security Issue in Intel's Active Management Technology (AMT)," Jan ۲۰۱۸, https://business.f-secure.com/intel-amt-security-issue.

[۴].M. Rouse, "Evil Maid Attack," Jan ۲۰۱۸, http://searchsecurity.techtarget.com/definition/evil-maid-attack.

[۵]."Evil Maid Attacks on Encrypted Hard Drives," https://www.schneier.com/blog/archives/۲۰۰۹/۱۰/evil_maid_attac.html.

[۶]."Evil Maid goes after TrueCrypt!," Oct ۲۰۰۹, http://theinvisiblethings.blogspot.com/۲۰۰۹/۱۰/evil-maid-goes-after-truecrypt.html.

[۷].A. L. Williams, "Bios Change for Dell ۷۵۵ & ۹۶۰," Sep ۲۰۱۰, https://wikispaces.psu.edu/pages/viewpage.action?pageId=٦٢٤٢٣٦١٧.

[۸].C. Allgemien, "Dell T۲۰ – Intel AMT aktivieren und per KVM fernsteuern," Arm, March ۲۰۱۷, https://goneuland.de/wordpress/dell-t۲۰-intel-amt-aktivieren-und-per-kvm-fernsteuern/.