عنوان:

پروژه‌ی زیرو گوگل: پیشگام امنیت سایبری از طریق تحقیق بر روی آسیب‌پذیری‌های روز صفر

۱. مقدمه

پروژه‌ی زیرو گوگل یک ابتکار ویژه در حوزه امنیت سایبری است که در سال ۲۰۱۴ ایجاد شده و مأموریت اصلی آن شناسایی و کاهش آسیب‌پذیری‌های روز صفر است .نقاط ضعفی که ناشناخته‌اند و هیچ اصلاحی برای آن‌ها وجود ندارد. این آسیب‌پذیری‌ها، زمانی که کشف و توسط بازیگران مخرب مورد سوءاستفاده قرار می‌گیرند، می‌توانند تهدیدات جدی برای افراد، کسب‌وکارها و دولت‌ها ایجاد کنند. هدف پروژه‌ی زیرو افزایش امنیت کلی نرم‌افزارها در فضای فناوری از طریق کشف این نقص‌ها قبل از اینکه مهاجمان بتوانند از آن‌ها سوءاستفاده کنند، می‌باشد و به این ترتیب، ایمنی کاربران در سطح جهانی را افزایش می‌دهد.

۲. مأموریت و اهداف

اهداف اصلی پروژه‌ی زیرو عبارتند از:

- **شناسایی و کاهش آسیب‌پذیری‌های روز صفر** :آسیب‌پذیری‌های روز صفر به عنوان هدف‌هایی مورد توجه مهاجمان هستند، زیرا تا زمانی که ناشناخته باقی بمانند، می‌توانند مورد سوءاستفاده قرارگیرند. پروژه‌ی زیرو تلاش می‌کند تا این آسیب‌پذیری‌ها را قبل از اینکه به دست مهاجمان بیفتند، شناسایی کند.
- **تنظیم استانداردهای افشای آسیب‌پذیری** :پروژه‌ی زیرو از افشای مسئولانه آسیب‌پذیری‌ها حمایت می‌کند و به این ترتیب شرکت‌ها را به رفع سریع‌تر نقص‌ها ترغیب می‌کند. این رویکرد به ایجاد استانداردهای صنعتی در زمینه زمان‌بندی افشای آسیب‌پذیری‌ها کمک کرده است.
- **افزایش آگاهی و بهبود شیوه‌های امنیتی در صنعت** :از طریق افشای عمومی و تحقیقات مستمر، پروژه‌ی زیرو سعی دارد شرکت‌ها را به اتخاذ شیوه‌های امنیتی پیشگیرانه ترغیب کند.

۳. ساختار تیم و اعضای کلیدی

پروژه‌ی زیرو به‌طور مستقل از سایر تیم‌های امنیتی گوگل فعالیت می‌کند و شامل محققان امنیتی مشهور است که در زمینه‌های تجزیه و تحلیل سیستم، مهندسی معکوس و بهره‌برداری از آسیب‌پذیری‌ها تخصص دارند. اعضای برجسته تیم عبارتند از:

- **تاویس اورمندی** :او به خاطر کشف آسیب‌پذیری‌ها در نرم‌افزارهای پرکاربرد شناخته شده است، از جمله محصولات آنتی‌ویروس و مدیران رمزعبور.
- **ناتالی سیلوانوویچ** :متخصص امنیت برنامه‌های پیام‌رسان است و نقص‌های متعددی را در برنامه‌های ارتباطی محبوب شناسایی کرده است.

- **ایان بیر**:او به خاطر کارهایش بر روی امنیت iOS و macOS مشهور است و به آگاهی از آسیب‌پذیری‌های جدی در این سیستم‌عامل‌ها کمک کرده است.

هر یک از این اعضا دارای تجربه‌های گسترده‌ای از پروژه‌های امنیتی در سطح بالا هستند که به تیم اجازه می‌دهد به‌طور مستقل کار کند و نرم‌افزارها را بدون توجه به ارتباط آن‌ها با گوگل بررسی کند. این رویکرد به حداکثر رساندن مزایای امنیتی در سطح صنعت کمک می‌کند.

۴ .تکنیک‌های تحقیق و روش‌های کلیدی

محققان پروژه‌ی زیرو از تکنیک‌ها و ابزارهای پیشرفته برای کشف آسیب‌پذیری‌ها استفاده می‌کنند:

- **فازی(Fuzzing)** : روشی که ورودی‌های تصادفی یا غیرمنتظره را به نرم‌افزار وارد می‌کند تا پاسخ‌های غیرمعمول را تحریک کند و به این ترتیب نقص‌های امنیتی پنهان را شناسایی کند. پروژه‌ی زیرو ابزارهایی مانند *Syzkaller*، یک فازر برای هسته لینوکس، را توسعه داده است که قابلیت‌های آزمایش فازی را بهبود می‌بخشد.
- **مهندسی معکوس** :محققان بدون دسترسی به کد منبع، کد کامپایل شده را تحلیل می‌کنند تا بفهمند نرم‌افزار چگونه عمل می‌کند و به این ترتیب نقاط ضعف را شناسایی کنند.
- **تحلیل باینری و بررسی‌های دستی کد**: با بررسی دستی کد باینری، محققان می‌توانند آسیب‌پذیری‌هایی را کشف کنند که ابزارهای خودکار ممکن است از آن‌ها غافل شوند. این فرآیند وقت‌گیر است اما در شناسایی نقص‌های پیچیده بسیار مؤثر بوده است.
- **توسعه بهره‌برداری** :برای ارزیابی شدت آسیب‌پذیری، محققان ممکن است نمونه‌های اثبات مفهوم proof-of-concept ایجاد کنند. این کمک می‌کند تا تأثیر بالقوه را ارزیابی کرده و پیشنهادات خاصی برای کاهش خطرات ارائه دهند.
- **توسعه ابزار**:پروژه‌ی زیرو ابزارهای مختلفی ایجاد کرده که به‌صورت عمومی در دسترس جامعه تحقیقاتی قرار دارند.این ابزارها قابلیت‌های پیشرفته‌ای برای کشف آسیب‌پذیری‌ها ارائه می‌دهند و به تسهیل تحقیقات امنیتی در این حوزه کمک می‌کنند.

۵ .سیاست افشا و تأثیر آن

سیاست افشای ۹۰ روزه

پروژه‌ی زیرو از یک **سیاست افشای ۹۰ روزه** برای آسیب‌پذیری‌ها پیروی می‌کند:

- پس از کشف یک آسیب‌پذیری، پروژه‌ی زیرو به‌طور محرمانه آن را به تولیدکننده گزارش می‌دهد و یک دوره ۹۰ روزه برای انتشار یک اصلاحیه به آن‌ها می‌دهد.
- اگر در این مدت اصلاحیه‌ای منتشر نشود، پروژه‌ی زیرو به‌طور عمومی آسیب‌پذیری را افشا می‌کند و به کاربران اطلاع می‌دهد تا اقداماتی پیشگیرانه انجام دهند.
- در مواردی که تولیدکنندگان پیشرفت قابل توجهی نشان دهند، پروژه‌ی زیرو ممکن است مهلت را به مدت ۱۴ روز تمدید کند.

این سیاست باعث شده است تا شرکت‌ها مجبور به اتخاذ چرخه‌های پچ سریع‌تر شوند، اگرچه گاهی اوقات با انتقاداتی از سوی تولیدکنندگان مواجه می‌شود که احساس می‌کنند تحت فشار برای انتشار اصلاحیه‌های سریع قرار دارند.

تأثیر بر استانداردهای صنعتی

- **تشویق به چرخه‌های پچ سریع‌تر**:سیاست ۹۰ روزه استاندارد جدیدی را تعیین کرده و شرکت‌ها را به اولویت دادن به پچ‌ها و امنیت ترغیب کرده است.
- **شفافیت**: أکید پروژه‌ی زیرو بر افشای عمومی (پس از مهلت) استانداردی برای شفافیت در مورد آسیب‌پذیری‌ها تعیین کرده و به کاربران قدرت می‌دهد تا کنترل امنیت خود را به دست بگیرند.

۶. دستاوردهای مهم و تأثیرات آن‌ها

پروژه‌ی زیرو تأثیر قابل‌توجهی بر امنیت نرم‌افزارها گذاشته و آسیب‌پذیری‌های مهمی را در محصولات پرکاربرد شناسایی و افشا کرده است. برخی از کشفیات مهم عبارتند از:

- **آسیب‌پذیری‌های Meltdown و Spectre** : در سال ۲۰۱۸، پروژه‌ی زیرو آسیب‌پذیری‌هایی را در معماری‌های پردازنده که بر روی پردازنده‌های Intel ، AMD و ARM تأثیر می‌گذاشت، افشا کرد. این نقص‌ها به مهاجمان اجازه می‌دادند به داده‌های حساس دسترسی پیدا کنند و این باعث اقدامات گسترده‌ای در صنعت سخت‌افزار و نرم‌افزار برای کاهش خطرات شد.
- **آسیب‌پذیری‌های جاسوسی Pegasus**: پروژه‌ی زیرو آسیب‌پذیری‌هایی را شناسایی کرد که توسط جاسوس‌افزار Pegasus گروه NSO استفاده می‌شد و برای هدف قرار دادن فعالان حقوق بشر و خبرنگاران به کار می‌رفت. این کشف به اهمیت امنیت قوی برای پلتفرم‌های iOS و Android تأکید کرد.
- **آسیب‌پذیری‌های ویندوز و کروم** :پروژه‌ی زیرو نقص‌های مهمی را در ویندوز مایکروسافت، گوگل کروم و دیگر نرم‌افزارهای محبوب گزارش کرده است که به بهبودهای امنیتی قابل‌توجهی در سیستم‌عامل‌ها و مرورگرهایی که میلیاردها نفر از آن‌ها استفاده می‌کنند، منجر شده است.

این کشفیات موجب انتشار به‌روزرسانی‌های امنیتی شده که بر روی میلیون‌ها کاربر تأثیر گذاشته و اصلاحات امنیتی وسیعی را در شرکت‌های متأثر به همراه داشته است.

۷. چالش‌ها و جنجال‌ها

سیاست ۹۰ روزه و جنجال‌های آن

- مهلت سخت‌گیرانه ۹۰ روزه به‌عنوان موضوعی جنجالی مطرح شده است، زیرا برخی از تولیدکنندگان بر این باورند که این سیاست می‌تواند منجر به پچ‌های شتابزده یا آزمایش‌نشده شود که ممکن است خطرات جدیدی را به همراه داشته باشد.
- زمانی که افشای عمومی قبل از در دسترس قرار گرفتن پچ انجام شود، کاربران را در معرض خطر قرار می‌دهد، همان‌طور که در موارد *Spectre* و *Meltdown* دیده شد.

روابط با تولیدکنندگان نرم‌افزار

- رویکرد مستقل پروژه‌ی زیرو گاهی اوقات روابط با تولیدکنندگان را تحت‌فشار قرار می‌دهد، زیرا آن‌ها احساس می‌کنند مجبور به اولویت دادن به پچ‌ها هستند. درحالی که برخی از شرکت‌ها این سیاست را پذیرفته‌اند، برخی دیگر با مهلت‌های سخت آن مخالفت می‌کنند.

توازن امنیت و ملاحظات اخلاقی

- پروژه‌ی زیرو با ملاحظات اخلاقی روبه‌رو است، به‌خصوص زمانی که آسیب‌پذیری‌ها در سناریوهای حمله فعال یافت می‌شوند. در چنین مواردی، آن‌ها باید مزایای افشای عمومی را در برابر خطرات ناشی از افشای کاربران به سوءاستفاده‌های بیشتر بسنجند.

۸. تأثیر و میراث گسترده‌تر در صنعت

کار پروژه‌ی زیرو به‌طور عمیق استانداردهای امنیت سایبری در صنعت فناوری را تحت تأثیر قرار داده است:

- **افزایش آگاهی امنیتی** :یافته‌های آن‌ها به‌طور قابل‌توجهی آگاهی درباره آسیب‌پذیری‌های روز صفر را افزایش داده و شرکت‌ها را به اتخاذ شیوه‌های امنیتی بهبود یافته ترغیب کرده است.
- **تأثیر بر استانداردهای افشا** : بسیاری از سازمان‌ها استانداردهای مشابهی را برای زمان‌بندی افشای آسیب‌پذیری‌ها پذیرفته‌اند که نشان‌دهنده تأثیر پروژه‌ی زیرو بر هنجارهای صنعتی است.
- **بهبود توسعه نرم‌افزار**:توسعه‌دهندگان به‌طور فزاینده‌ای شیوه‌های امنیتی را در مراحل اولیه چرخه توسعه گنجانده و برخی شرکت‌ها تیم‌های تحقیقاتی با مدلی مشابه پروژه‌ی زیرو تأسیس کرده‌اند.

۹. نتیجه‌گیری

پروژه‌ی زیرو گوگل یک رویکرد پیشگامانه به تحقیق در حوزه آسیب‌پذیری‌ها را نمایان می‌کند. تمرکز آن بر شناسایی، افشا و ارتقاء رفع آسیب‌پذیری‌های روز صفر، محیط دیجیتال را برای میلیون‌ها نفر در سرتاسر جهان ایمن‌تر کرده است. با وجود چالش‌های مربوط به زمان‌بندی افشای اطلاعات و روابط با تولیدکنندگان، کار پروژه‌ی زیرو به تعیین استانداردهای جدید برای امنیت و شفافیت کمک کرده و به بهبود تاب‌آوری نرم‌افزارها و افزایش آگاهی عمومی از خطرات امنیت سایبری منجر شده است. این ابتکار به پیشبرد شیوه‌های امنیتی ادامه خواهد داد و الهام‌بخش تلاش‌های مشابه در صنعت فناوری خواهد بود.