بسمه تعالی

مرکز ماهر

مرکز مدیریت امداد و هماهنگی
عملیات رخدادهای رایانه‌ای
سازمان فناوری اطلاعات ایران
معاونت امنیت فضای تولید و تبادل اطلاعات

آسیب‌پذیری در آنتی‌ویروس Bitdefender و اجرای کد مخرب از راه دور

خبر آسیب‌پذیری

شناسه سند ..... Maher_13990407-2
نوع سند ..... گزارش فنی
شماره نگارش ۰,۱
تاریخ نگارش ۱۳۹۹/۰۴/۰۵
طبقه‌بندی سند ..... عادی

تهران، میدان آرژانتین، ابتدای بلوار بیهقی، نبش خیابان شانزدهم، ساختمان شماره ۱، سازمان فناوری اطلاعات ایران

(۰۲۱) ۴۲۶۵۰۰۰۰ (۰۲۱) ۴۲۶۵۰۰۰۰ cert.ir

فهرست مطالب

۱ خلاصه

به تازگی یک آسیب‌پذیری در آنتی‌ویروس Bit Defender مشاهده شده است که به واسطه آن، هکرها می‌توانند کدهای مخرب خود را از راه دور اجرا کنند. این آسیب‌پذیری با شناسه "CVE-2020–8102"، نسخه بروزرسانی اخیر آنتی‌ویروس Bit Defender را تحت‌تأثیر قرار داده است. علاوه براین، محققان مدعی هستند که این آسیب‌پذیری اثرات خطرناک و قدرتمندی را به دنبال دارد چراکه آنتی‌ویروسی را مورد حمله قرار داده است، که معمولا توسط کاربران مختلفی برای حفاظت از دستگاه‌های خود استفاده می‌شود. این آنتی‌ویروس در بین کاربران ایرانی نیز محبوبیت زیادی دارد و لازم است که کاربران این آنتی‌ویروس نسبت به آسیب‌پذیری کشف شده آگاهی کامل داشته و نسبت بروزرسانی آن اقدام نمایند.

۲ جزئیات آسیب‌پذیری

به گفته محققان، آسیب‌پذیری مذکور به دلیل اعتبارسنجی نادرست ورودی در مرورگر Safepay است که عنصری از Bitdefender Total Security 2020 می‌باشد(در بخش **محصول تحت‌تأثیر**، در خصوص جزئیات مرورگر Safepay بیشتر توضیح داده خواهد شد). به سبب این آسیب‌پذیری، یک صفحه وب خارجی و ساختگی قادر است دستورات را از راه دور در فرآیند Safepay Utility اجرا کند. بر اساس ادعای محققان، آسیب‌پذیری ذکر شده نسخه‌های 24.0.20.116 آنتی‌ویروس Bitdefender Total Security 2020 را تحت‌تأثیر قرار داده است. این آنتی‌ویروس، اتصالات امن HTTPS را بررسی می‌کند و بنا به دلایلی ترجیح می‌دهد از نمایش صفحات خطای[۱] مربوط به خود استفاده کند و با آثار مخرب کمتر، در این مورد شبیه به نحوه عملکرد آنتی‌ویروس Kaspersky می‌باشد.

این آسیب‌پذیری توسط Wladimir Palant، توسعه‌دهنده AdBlock Plus افشا شد. وی از یک وب‌سرور محلی و یک SSL معتبر استفاده کرد که در مدت کوتاهی، آن را با مقدار نامعتبری تغییر داد. Palant این رفتار را از طریق PoC نشان داد که در آن یک وب‌سرور در حال اجرا داشت که گواهی SSL معتبر را بر روی اولین درخواست ارائه می‌داد اما بلافاصله به یک مقدار نامعتبر تبدیل می‌شد.

جزئیات آسیب‌پذیری به شرح زیر است:

[۱] error pages

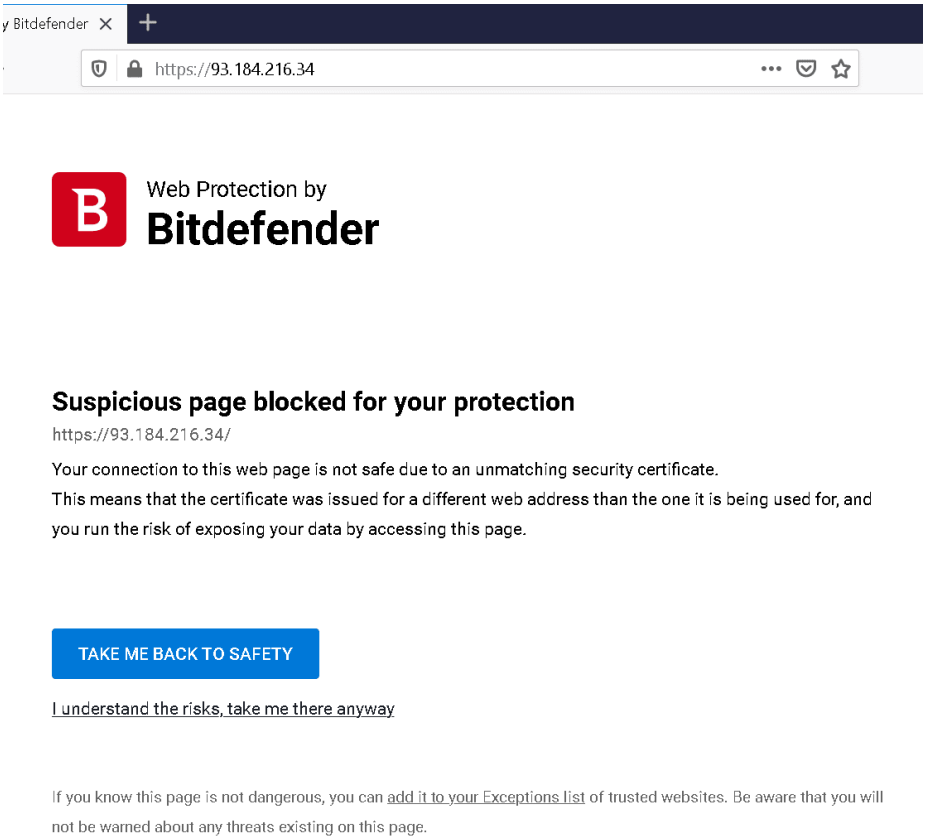
CVE ID: CVE-2020-8102

CVSS score: 8.8

Affected vendors: Bitdefender

Affected products: Bitdefender SafePay

این مورد مشخص، مربوط به آنتی‌ویروس Kaspersky با روش‌های ورودی مشابه است، اما وب‌سایت‌ها نیز می‌توانند به راحتی برخی از توکن‌های امنتی صفحات خطا را بدست آورند.



شکل ۱ نمایی از مرورگر Safepay

این توکن‌های امنیتی نمی‌توانند جهت لغو خطاها در دیگر وب‌سایت‌ها استفاده شوند، اما می‌توان از آن‌ها جهت شروع اجماع[۱] با مرورگر Safepay مبتنی بر Chromium استفاده کرد. براساس گزارش Bitdefender Advisory، API هیچگاه جهت پذیرش داده‌های غیرقابل اعتماد درنظرگرفته نشده است و با همان آسیب‌پذیری که قبلاً کارشناسان امنیتی در Avast Secure Browser مشاهده کردند، مورد حمله قرار می‌گیرد.

[۱] assembly

در این حالت مهاجم می‌تواند به راحتی پرچم‌های خط فرمان[۱] را درج کرده و باعث شود اپلیکیشنِ دلخواه، کار خود را شروع کند.

۳ محصول تحت‌تأثیر

Bitdefender Safepay محصول تحت‌تأثیر این آسیب‌پذیری می‌باشد، این نرم‌افزار امنیت حریم خصوصی شما در زمان انجام عملیات بانکی و پرداخت های آنلاین را تضمین می‌کند و به صورت یک دسکتاپ ثانویه که بر پایه مرورگر گوگل کروم می‌باشد عمل می‌کند. هنگام استفاده از این نرم‌افزار، معاملات آنلاین شما در برابر کی‌لاگرها، صفحات فیشینگ و تروجان‌ها محافظت می‌شود و با خیال راحت می‌توانید عملیات بانکی خود را انجام دهید. این نرم‌افزار به صورت اتوماتیک تمامی نرم‌افزارهای دسکتاپ را غیر فعال می‌کند و حتی اجازه عکس گرفتن از دسکتاپ توسط نرم‌افزارهای جاسوسی و حتی کیبورد را نمی‌دهد.

۴ اکسپلویت آسیب‌پذیری در وب‌سایت‌های بانکی[۲]

Bitdefender الگوهایی را ارائه می دهد که حاکی از چگونگی تولید کد تزریق شده در وب‌سایت بانکی می‌باشد.

```
var params = encodeURIComponent(window.location);
sid = "" + Math.random();
obj_ajax.open("POST", sid, true);
obj_ajax.setRequestHeader("Content-type", "application/x-www-form-urlencoded");
obj_ajax.setRequestHeader("BDNDSS_B67EA559F21B487F861FDA8A44F01C50", "{%NDSECK%}");
obj_ajax.setRequestHeader("BDNDCA_BBACF84D61A04F9AA66019A14B035478", "{%NDCA%}");
obj_ajax.setRequestHeader("BDNDWB_5056E556833D49C1AF4085CB254FC242", "{%OBKCMD%}");
obj_ajax.setRequestHeader("BDNDOK_4E961A95B7B44CBCA1907D3D3643370D", "{%OBKREFERRER%}");
obj_ajax.send(params);
```

گفتنی است که این الگوها دیگر مورد استفاده قرار نمی‌گیرند، اما راهی برای دسترسی به وب‌سایت مخرب در مرورگر Safepay وجود دارد که در رابطه با وب‌سایت‌های بانکداری که به درستی از هم تفکیک شده‌اند، می‌تواند مورد بررسی قرار گیرد.

---

[۱] command-line

[۲] Banking Mode

۵ راه حل

Bitdefender در حال بررسی این آسیب‌پذیری می‌باشد، آن‌ها یک بروزرسانی خودکار را نصب کرده‌اند که آسیب‌پذیری مذکور را در نسخه 24.0.20.116 و تمامی نسخه‌های بعدیش، رفع می‌کند، پس با توجه به اهمیت این موضوع، هر چه سریع‌تر تنظیمات بروزرسانی آنتی‌ویروس خود را بررسی کنید.

۶ جمع‌بندی

اخیراً یک آسیب‌پذیری با شناسه "CVE-2020–8102" در محصول BitDefender Total Security 2020 شرکت BitDefender کشف شده است که از نوع اجرای کد مخرب از راه دور بوده و در اثر اعتبارسنجی نادرست ورودی در مرورگر Safepay به وجود آمده است، از آنجا که آنتی‌ویروس‌ها جهت حفظ ایمنی دستگاه استفاده می‌شوند و اگر مورد حمله هکرها قرار گیرند، می‌توانند خسارات جبران‌ناپذیری را رقم زنند، لازم است هر چه سریع‌تر اقدامات لازم را در این خصوص مبذول نمایید.

۷ منابع

https://gbhackers.com/vulnerability-in-bitdefender-anti-virus/

https://www.bitdefender.com/news/bitdefender-launches-free-safepay-standalone-to-protect-ebanking-shopping-2790.html

https://sensorstechforum.com/cve-2020-8102-bitdefender/