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 رخداد اختلال در سیستم‌های عامل ویندوز به واسطه CrowdStrike

## گزارش فنی

| | |
|---|---|
| شناسه‌سند..... | Incident_CrowdStrike_14030430 |
| نوع سند ..... | گزارش ..... |
| شمارهنگارش..... | ۱ ..... |
| تاریخ‌نگارش..... | ۱۴۰۳/۰۴/۳۰ ..... |
| | عادی ..... |

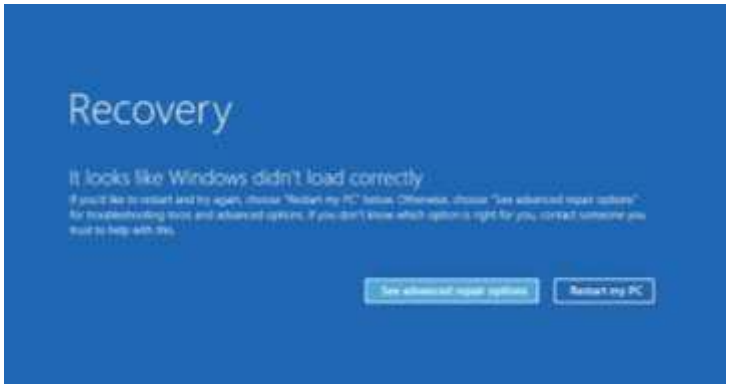
تهران، خیابان شهید بهشتی- بین بزرگراه شهید مدرس و خیابان احمد قصیر- پلاک۲۶۷

cert.ir (۰۲۱) ۸۸۱۱۵۷۲۴ (۰۲۱) ۸۸۱۱۵۷۲۴

## فهرست مطالب

# ۱ مقدمه

وجود نقصی در آپدیت ارائه شده برای سنسور CrowdStrike Falcon باعث نمایش مکرر صفحه آبی (BSOD) و عدم بارگذاری سیستم‌عامل در سیستم‌های مبتنی بر مایکروسافت ویندوز و در نتیجه ایجاد اختلال در بسیاری از سیستم‌های استفاده کننده از این پلتفرم در سراسر جهان شده است.




**شکل ۱. صفحه‌ی آبی مرگ**

# ۲ شرح رخداد

صبح روز جمعه، گزارشات متعددی از اقصی نقاط جهان مبنی بر وقوع خطای BSOD (خطای صفحه آبی یا سبز در سیستم‌های عامل ویندوز) منتشر شد. با وقوع این خطا، سیستم‌های عامل بطور کامل از کار افتاده و با راهاندازی مجدد نیز،سیستم عامل بوت نمی‌گردد. اطلاعات تکمیلی نشان داد این خطا بر اثر انتشار یک بروزرسانی معیوب بر روی محصول امنیت سایبری شرکت آمریکایی CrowdStrike به وقوع پیوسته است.

طبق بررسی‌های انجام شده توسط مراکز مستقل و همچنین اعلام مدیران شرکت CrowdStrike، این حادثه بر اثر انتشار یک بروزرسانی معتبر از سوی این شرکت در رابطه با محصول این شرکت با نام Falcon بوده است. در بروزرسانی منتشر شده، یک درایور معیوب مرتبط با Falcon Agent به سیستم‌ها منتقل شده و باعث این اختلال گشته است. این حادثه صرفا به دلیل خطای انسانی و ضعف در کنترل کیفی محصول و همچنین عدم اعمال فرایند مناسب ارزیابی و مدیریت انتشار بروزرسانی بوده است.

از سوی دیگر بر اساس گزارشات، با توجه به استفادهی گسترده از این محصول در زیرساخت پلتفورم ابری مایکروسافت (Azure) اختلال جدی در عملکرد و خدمت رسانی آن مشاهده شده است. این دو اختلال همزمان، منجر به وقوع اختلالات جدی در سراسر جهان شده است.

# ۳ راهکار رفع در حال حاضر

در صورت استفاده از پلتفرم CrowdStrike Falcon توصیه می‌شود از نصب به روزرسانی ارائه شده در تاریخ ۲۰۲۴/۰۷/۱۹ معادل با ۱۴۰۳/۰۴/۲۹ خودداری گردد و امکان آپدیت خودکار نیز تا رفع مشکل و ارائه راهکار توسط ارائه دهندگان این سرویس غیرفعال باشد.

فعلا بازگردانی سیستم‌های آسیب دیده تنها به صورت فیزیکی و با استفاده از مراحل ارائه شده در راهکارهای زیر امکان است:

۱- بوت ویندوز از طریق SafeMode یا Windows Recovery Environment (WRE)

۲- رفتن به مسیر C:\Windows\System32\drivers\CrowdStrike

۳- حذف فایل C-00000291*.sys

۴- راهاندازی مجدد و بوت ویندوز در حالت عادی

# ۴ بررسی امکان بروز مشکل در کشور

با وجود تاثیرات و اختلالات گسترده در بسیاری از فرودگاهها و لغو بسیاری از پروازهای خطوط هوایی و آسیب به بانک‌ها، مراکز و سازمانهای بزرگ و مهم در بسیاری از کشورها، تاکنون گزارشی از اختلال در هیچ یک از زیرساخت‌ها و خدمات ارائه شده در ایران دریافت نشده است.

با توجه به تحریم اعمالی از سوی هر دو شرکت CrowdStrike و محصول Azure مایکروسافت بر ایران، تقریبا هیچ استفادهای از این دو محصول در کشور ما صورت نمی‌گیرد. این موضوع باعث شده وقوع اختلالات فوق الذکر، کشور ما را با مشکلی مواجه نکند.