CTI Jelentés

A 2024-es CrowdStrike incidens elemzése

NEMZETI KIBERBIZTONSÁGI INTÉZET

Tartalomjegyzék

Bevezetés

2024. július 19-én a globális digitális infrastruktúra egyik legsúlyosabb működési válságát élte át, amikor a CrowdStrike Falcon végpontvédelmi platform hibás frissítése következtében több millió Windows-alapú rendszer összeomlott. Az incidens nem csupán technikai hiba volt, hanem komplex működésbiztonsági és architekturális gyengeségek láncreakciójának következménye, amely rövid idő alatt repülőterek, kórházak, vállalatok és állami intézmények leállásához vezetett világszerte.

A rendkívüli esemény példátlanul széleskörű IT-infrastruktúra kimaradást eredményezett, amelyre a szakirodalomban korábban legfeljebb szcenárióalapú becslések léteztek, például az Y2K-válság idején. A kialakult helyzet sok tekintetben megfelelt a szakmában gyakran csak „kiberarmageddonként" emlegetett, elméleti forgatókönyveknek, amelyek szerint egyetlen rosszul kezelt frissítés globális szintű dominóhatást válthat ki.

A jelen tanulmány célja, hogy részletes technikai magyarázatot adjon a hibás frissítés okairól, a kernel-szintű működés kritikus sajátosságairól, valamint átfogó képet nyújtson a kialakult kár mértékéről, a helyreállítási folyamatokról, és a hibát követő iparági változásokról. Az eset nem csupán egy szoftverhiba következménye volt, hanem komoly tanulságokkal szolgál a modern végpontvédelem, a frissítésmenedzsment és az automatizált tesztelés biztonsági kockázatairól.

Mi az a CrowdStrike Falcon?

A CrowdStrike Falcon egy felhőalapú végpontvédelmi platform, amelyet kifejezetten vállalati szintű informatikai infrastruktúrák proaktív védelmére fejlesztettek ki. A rendszer az úgynevezett EDR (Endpoint Detection and Response) technológiai osztályba tartozik, amely túllép a hagyományos antivírus megközelítésen: valós idejű viselkedéselemzéssel, anomáliadetektálással és incidenskezelési képességekkel támogatja a szervezetek kiberbiztonsági védelmét.

A modern fenyegetések – például zero-day exploitok, célzott APT-kampányok vagy késleltetett kódvégrehajtási technikák – olyan komplexitást képviselnek, amelyek ellen a szignatúraalapú vírusvédelem önmagában elégtelen. A Falcon architektúrája erre válaszul valós időben gyűjt és továbbít telemetriai adatokat a CrowdStrike felhőplatformjára, ahol gépi tanulási algoritmusok értékelik az eseményeket, és azonosítják az atipikus vagy kártékony viselkedési mintázatokat.

A Falcon egyik legnagyobb előnye az, hogy a detekciós logika jelentős része nem helyben, hanem a CrowdStrike infrastruktúráján belül fut, így a végpontokon minimális erőforrásigénnyel, mégis naprakész és skálázható védelmet képes nyújtani. Ez a felhő-kliens architektúra ugyanakkor kritikus függőségeket is létrehoz, amelyek egy-egy hibás definíciós frissítés esetén tömeges hatásokat válthatnak ki, ahogyan az a 2024-es incidens során is történt.

A Falcon platform moduláris felépítésű, lehetővé téve, hogy a szervezetek a biztonsági érettségük és igényeik alapján különféle komponenseket – például Prevent, Insight, OverWatch, Discover, X, Search Engine, Horizon, Cloud Workload Prot – kapcsoljanak be.

A Falcon Complete csomag tartalmazza az automatikus válaszadást és a menedzselt észlelési szolgáltatásokat is, ezáltal teljes körű védelmet biztosít a végponti támadási lánc minden szakaszában.

Míg a hagyományos antivírus szoftverek szignatúraalapú felismerést alkalmaznak – azaz ismert kártevőminták alapján azonosítanak fenyegetéseket –, a Falcon dinamikus, viselkedésalapú és prediktív modellalkotással működik. Ennek köszönhetően képes ismeretlen, polimorf vagy obfuszkált támadások detektálására is, amelyek a hagyományos eszközökön gyakran észrevétlenül átsiklanának.

Lényeges különbség továbbá, hogy a Falcon szolgáltatásként működő védelmet nyújt: a kritikus detekciós és döntési folyamatok a felhőben zajlanak, nem pedig a kliens gépen. Ez nemcsak teljesítményelőnyt és jobb frissítési hatékonyságot jelent, hanem a rendszerszintű frissítések központosított terjesztését is lehetővé teszi, ami kulcsszerepet játszott a globális szintű leállás kialakulásában.

Kernel és felhasználó mód

A modern operációs rendszerek architektúrájának alapvető biztonsági és stabilitási pillére a kernel és a felhasználói mód elkülönítése. Ez a szétválasztás biztosítja, hogy az alkalmazások ne férhessenek hozzá közvetlenül a hardvererőforrásokhoz, a rendszer memóriájához vagy más kritikus komponensekhez, ezzel minimalizálva a véletlenszerű vagy rosszindulatú beavatkozás lehetőségét.

Az x86 architektúra például négy különálló jogosultsági szintet (Ring) definiál, ahol a Ring 0 a legmagasabb privilégiumszintet – azaz kernel módot – képviseli, míg a Ring 3 a legalacsonyabb szintű, felhasználói módú programok futtatási környezete. A kernel módban működnek az operációs rendszer magkomponensei, az eszközillesztők (driverek) és más kritikus szolgáltatások, amelyek közvetlen hardvereléréssel, memóriakezeléssel és folyamatütemezéssel foglalkoznak.

A felhasználói módú alkalmazások kizárólag az operációs rendszer által biztosított interfészeken (API-kon és rendszerhívásokon) keresztül képesek szolgáltatásokat igénybe venni. Minden olyan művelet – például fájlhozzáférés, hálózati kommunikáció vagy memóriaművelet –, amely kernel beavatkozást igényel, rendszerhívás (syscall) útján történik, amely során a vezérlés átvált a kernel kódjára, majd visszatér a felhasználói térbe a művelet befejeztével.

A kernel módú kód jogosultsága teljes körű, hozzáfér az összes memóriacímhez, rendszerfolyamathoz és hardvereszközhöz. Ezért minden kernel szinten futtatott komponens – például egy illesztőprogram – kockázati szempontból a legmagasabb szintű bizalmi zónába tartozik.

E komponensek bármilyen logikai vagy memóriakezelési hibája az egész rendszer instabilitását vagy azonnali leállását okozhatja, jellemzően BSoD („Blue Screen of Death") formájában.

A CrowdStrike incidens pontosan ezt a kockázatot demonstrálta: egy kernel módú komponens – a Falcon illesztőprogram – egyetlen hibás memóriaművelete elegendő volt ahhoz, hogy a Windows operációsrendszer működésképtelenné váljon. Ez nem egyedi Windows-jelenség: minden modern operációs rendszer (Linux, macOS, BSD) hasonló önvédelmi mechanizmusokat alkalmaz, amelyek kernelhibák esetén automatikusan leállítják a rendszert a további adatsérülések vagy kompromittálódás megelőzése érdekében.

Annak érdekében, hogy a kernel módú komponensek megbízhatósága ellenőrizhető legyen, a Microsoft WHQL (Windows Hardware Quality Labs) aláírási rendszerén keresztül hitelesíti azokat az illesztőprogramokat, amelyek a Windows rendszerrel együtt vagy azon belül kívánnak működni. Egy WHQL-tanúsítvánnyal rendelkező driver olyan validációs folyamatokon megy keresztül, amelyek elvileg minimalizálják a stabilitási kockázatokat. Ez azonban csak akkor érvényes, ha az aláírt komponens változatlan marad, és nem futtat dinamikusan betöltött, ellenőrizetlen logikát kernel módban – pontosan ez a szabály sérült meg a CrowdStrike hibás frissítésével.


CROWDSTRIKE

Mi okozta a problémát?

A CrowdStrike Falcon EDR-platform úgy épül fel, hogy a mélyreható, viselkedésalapú fenyegetésdetektálás érdekében kernel szintű átláthatósággal rendelkezzen. Ennek megvalósításához a Falcon komponensei között szerepel egy illesztőprogramként regisztrált szenzor, amely WHQL aláírással rendelkező kernelmodulként fut, noha nem fizikai hardvert vezérel, hanem a rendszerfolyamatok megfigyelésére és kiértékelésére szolgál. Ez az architektúra önmagában nem rendkívüli, hiszen több EDR-megoldás és például anti-cheat szoftver is hasonló jogosultsági modellel működik. A probléma azzal kezdődik, hogyan valósítják meg ezen komponensek dinamikus frissítését.

A kernel szintű illesztőprogramok módosítása normál esetben új WHQL-aláírást igényelne, amely idő- és erőforrás-igényes, több napos validációs ciklust jelent. A gyors reagálás és a friss fenyegetésekre való adaptív válaszadás érdekében a CrowdStrike olyan frissítési mechanizmust alkalmazott, amely a szenzorhoz tartozó logikai szabályokat és detekciós konfigurációkat külön fájlokban (ún. „channel file"-okban) tárolja. Ezek a fájlok nem képezik az illesztőprogram részét, így frissítésük nem igényli a WHQL-teszt megismétlését. A Falcon minden rendszerindításkor ellenőrzi a C:\Windows\System32\drivers\crowdstrike könyvtárat, és ha új channel fájlt talál, azt automatikusan betölti és értelmezi. Ezzel viszont aláíratlan, ellenőrizetlen konfigurációs logikát hajt végre kernel jogosultsági szinten.

2024. július 19-én UTC 04:09-kor a CrowdStrike kiadta a C-00000291.sys nevű új channel fájlt, amely a Falcon egyik belső modulját,

a Windows-named pipe kommunikációs csatornák elemzéséhez tartozó logikát frissítette. A frissítés célja a C2-infrastruktúrákhoz kötött pipe-használat detektálása volt, amely valódi biztonsági célokat szolgált. A kód azonban kritikus logikai hibát tartalmazott.

A detekciós mechanizmus három komponensből épült fel:

- A Template Type a szenzorba ágyazott sablonrendszer, amely meghatározza, milyen bemeneti paramétereket vár a detekcióhoz.
- A Content Interpreter a rendszerből származó eseményadatokat a Template logikája alapján értékeli ki.
- A Channel fájlok ezekhez adnak dinamikusan frissülő paraméterezést, így születnek meg a Template Instance-ok, azaz az élesben futó szabályok.

A 291-es channel fájl olyan szabályt adott át, amely 21 paramétert várt el a kiértékelés során, azonban a szenzor csak 20 paramétert továbbított a Content Interpreter felé. Az eltérés oka az volt, hogy a szenzorban futó integrációs kód nem volt frissítve a Template változásának megfelelően, így memórián kívüli (out-of-bounds) olvasási hibát eredményezett – egy tipikus CWE-125 típusú sebezhetőséget. A kernel ezt a hibát érzékelte, és biztonsági protokollként azonnal összeomlott (BSoD).

A helyzetet súlyosbította, hogy a Falcon szenzor rendszerindítási prioritással futott (registry „Start=1" értékkel), tehát a Windows operációs rendszer el sem indulhatott a hibás modul betöltése nélkül, így az újraindítás sem vezetett helyreállításhoz. Ez számos rendszernél végleges indulásképtelenséget okozott.


CrowdStrike
Outage
16:45

Felmerül a kérdés, hogy miért nem detektálták ezt a hibát még a kiadás előtt. A válasz a CrowdStrike belső tesztelőeszközében, a Content Validatorban keresendő, amely a frissítések automatikus verifikálását végezte. Mivel a korábbi szabályok a 21. paraméter helyén wildcard karaktereket használtak, a Content Validator soha nem észlelte, hogy az adott mező hiányzik, így a hibás logika látszólag minden validációs teszten átment. Ez egy klasszikus tesztautomatizálási csapda, ahol a rendszer nem arra vizsgál, amit feltételeznek, hanem arra, amit explicit ellenőriznek.

A hiba javítása

A CrowdStrike reagálása példaszerű gyorsasággal történt: alig 79 perccel a hibás frissítés közzététele után, UTC 05:27-kor a C-00000291.sys nevű channel fájlt globálisan visszavonták a tartalomterjesztési rendszerből. Ez a gyors intézkedés azt eredményezte, hogy azok az eszközök, amelyek még nem töltötték le a hibás fájlt, vagy csak ezután indultak újra, megúszták az összeomlást. Az automatikus frissítési pipeline-ból való eltávolítás megtörte a hibaterjedés exponenciális szakaszát, ugyanakkor már több millió rendszerre települt a sérült állomány.

Az érintett rendszerek helyreállítása manuális beavatkozást igényelt. Mivel a hibás driver kernel szinten, rendszerindításkor töltődött be, a szokványos bootfolyamat minden alkalommal összeomláshoz vezetett. A helyzetet az tette kezelhetővé, hogy a Falcon szenzor a Windows csökkentett módjában (Safe Mode) nem aktiválódott, így lehetőség nyílt az operációs rendszer korlátozott módú elindítására. Ebben a környezetben az üzemeltetők fizikai vagy távoli eléréssel eltávolíthatták a hibás állományt a C:\Windows\System32\drivers\crowdstrike\ könyvtárból.

Bár a javítás technikailag egyszerű volt – egyetlen fájl törlését jelentette –, a helyreállítási folyamat operatív szempontból sok esetben jelentős késedelmet szenvedett. Különösen a kritikus infrastruktúrák esetében (például repülőterek, egészségügyi rendszerek) gyakran belső szabályozási, auditálási és jogi protokollok akadályozták meg az azonnali beavatkozást. Az ilyen rendszerekhez való hozzáféréshez többszintű jóváhagyási lánc, szabályozott változásmenedzsment és auditálási kötelezettségek

társulnak, amelyek vészhelyzet esetén is lassíthatják a helyreállítást.

További nehézséget jelentett, hogy sok helyszínen hiányoztak a gyors beavatkozás feltételei – például fizikai hozzáférés, megfelelő technikai személyzet, vagy aktuálisan rendelkezésre álló helyreállítási eljárások. Egyes esetekben a rendszergazdák csak utólag, késleltetve értesültek a problémáról, és időre volt szükség, míg lokalizálták a hiba forrását.

Összességében a hiba javítása technológiai szinten gyorsan kivitelezhető volt, azonban az incidens rávilágított arra, mennyire sérülékenyek a helyi üzemeltetési folyamatok, ha a központosított szoftverfrissítés hibát tartalmaz, és nincs beépített mechanizmus a biztonságos rollbackre vagy self-healing funkcióra. A helyreállítás sebessége nem kizárólag technikai, hanem folyamat- és szervezeti érettségi kérdés is volt.

Az okozott kár

A CrowdStrike hibás frissítésének hatása példátlan globális informatikai zavart idézett elő, amely rövid idő alatt több mint 8,5 millió Windows-alapú eszköz leállásához vezetett. Ez a teljes globális Windows-ökoszisztéma mintegy 1%-át tette ki, és jól mutatja, hogy egy központosított frissítés hibája mekkora potenciális rendszerszintű kockázatot hordoz magában, különösen akkor, ha kernel szintű komponensről van szó.

A kritikus infrastruktúrák működésében bekövetkezett zavarok túlmutattak az IT-rendszereken, és fizikai szolgáltatások, logisztikai láncok, sürgősségi ellátások és állami műveletek működésképtelenségét is előidézték. A nemzetközi légiközlekedést például drasztikusan érintette az incidens: világszerte 5078 járat törlésére került sor – ez az aznapra tervezett összes járat 4,6%-át jelentette. A repülőterek check-in rendszerei, utasinformációs platformjai és háttérrendszerei – amelyek gyakran Windows-alapú munkaállomásokon és kiszolgálókon futnak – teljesen megbénultak.

A leállások földrajzi szempontból is kiterjedtek: Észak-Amerika, Európa, Ázsia és Ausztrália egyaránt érintett volt. A zavar több tucat légitársaságot sújtott, köztük európai és nemzetközi szereplőket, mint a Lufthansa, Wizz Air, KLM, Ryanair, Finnair és Turkish Airlines. A budapesti Liszt Ferenc Nemzetközi Repülőtér is több késést és járattörlést jelentett.

Az egészségügyi szektorban az incidens komoly műveleti zavarokat okozott: halasztható, de fontos kezelések és beavatkozások maradtak el, miközben sürgősségi rendszerek túlterhelődtek. Az Egyesült Államokban a 911-es hívószám több régióban ideiglenesen elérhetetlenné vált, ami rendkívül súlyos közegészségügyi kockázatot jelentett. Számos ország – köztük az USA, Kanada, Németország, Hollandia, Egyesült Királyság és Izrael – egészségügyi ellátórendszerei váratlan módon váltak részlegesen működésképtelenné, mivel az érintett munkaállomások nem tudtak csatlakozni az elektronikus nyilvántartásokhoz, diagnosztikai rendszerekhez vagy képalkotó eszközökhöz.

A dominóhatás elérte a banki, médiapiaci, energetikai, államigazgatási és ipari szektorokat is, ahol gyakran a termelési láncokat vagy a belső IT-szolgáltatásokat érték el a leállások. Mivel a vállalatok és intézmények figyelmét teljes mértékben a rendszerhelyreállítás kötötte le, kiberbűnözői csoportok tömeges social engineering és adathalász kampányokat indítottak, amelyek során CrowdStrike-támogatásnak vagy IT-helpdesknek álcázták magukat.

Ezek a kampányok belső jelszavak, VPN-kulcsok és távmenedzsment-eszközök kompromittálását célozták, sok esetben sikeresen. Elterjedtek a hamis e-mailek, csaló telefonhívások és hamis támogatási portálok, amelyek megtévesztették a válsághelyzetben működő munkatársakat. A megszokott védelmi vonalak, mint például az MFA vagy a helpdesk validáció, sok helyen nem működött vagy ideiglenesen ki lett kapcsolva, így a támadók alacsonyabb erőfeszítéssel tudtak sikeres kompromittálásokat végrehajtani.

A pénzügyi piac is reagált: a CrowdStrike részvényárfolyama 11%-ot esett az incidens napján, a Microsoft értéke pedig 1%-kal csökkent – utóbbi indokolatlanul, mivel a Windows rendszer rendeltetésszerűen működött, és a hibát teljes egészében a CrowdStrike frissítési logikája okozta. A közvélemény és az iparági bizalom számára azonban a valós technikai felelősség kevésbé volt átlátható, így a Microsoft is reputációs veszteséget szenvedett el.

A sérülés azért is kizárólag a Windows rendszereket érintette, mert a hibás channel fájl csak ezen platformra készült el. A Falcon Linuxon és macOS-en való integrációja eltérő mechanizmusokon alapul, így ezek az operációs rendszerek nem kapták meg a hibás frissítést, és nem is voltak érintettek az összeomlásban.

Utókövetés

A CrowdStrike válaszintézkedései az incidens után gyorsak, transzparensek és szervezettek voltak. A hibás frissítés visszavonása után a vállalat rövid időn belül részletes technikai tájékoztatót juttatott el ügyfeleihez, amely lépésről lépésre ismertette a manuális helyreállítási folyamatot. A cég vezetői nyilvánosan elismerték a hibát, és teljes felelősséget vállaltak az okozott károkért. George Kurtz vezérigazgató személyesen kért elnézést élő televíziós interjúban, demonstrálva ezzel a vállalat válságkommunikációs érettségét.

Bár a technikai károk mértéke jelentős volt, a CrowdStrike nem próbálta relativizálni az eset súlyát. A vállalat teljes technikai részletességgel közzétette a hiba kiváltó okait bemutató jelentést, amely egyaránt tartalmazta a hibás komponensek kapcsolatát, a tesztelési lánc hiányosságait, valamint a javításra tett intézkedések rendszerét. Ez a dokumentum 12 oldalas, nyilvánosan elérhető és példát mutatott arra, hogyan lehet az átláthatóságot bizalomerősítő eszközzé alakítani.

A CrowdStrike szimbolikus gesztusként kis értékű ajándékutalványokat (10 USD UberEats credit) küldött a szoftvert forgalmazó és ügyfeleket támogató partnerek egy részének, kifejezve elismerését a helyreállításban végzett munkájukért. Ugyanakkor ez a lépés vegyes fogadtatásban részesült, és több iparági szereplő szerint aránytalan volt az incidens súlyához képest – különösen, hogy az utalványok egy része technikai problémák miatt nem is volt beváltható.

A válság legfontosabb hozadéka a frissítési architektúra és disztribúciós modell teljes újratervezése lett. A CrowdStrike bejelentette, hogy ezentúl a tartalmi frissítések házon belüli, többszintű validációs folyamaton esnek át, mielőtt akár teszt-, akár éles rendszerekbe kerülnek. A kiadások több lépcsős, fokozatos terjesztésen keresztül zajlanak majd, lehetővé téve az esetleges hibák korai észlelését limitált környezetben. Az új rendszer három frissítési csatornát különböztet meg:

- Early adopter (azonnali hozzáférés, de nagyobb kockázat),
- General availability (stabil, széles körben elérhető verzió),
- Deferred update (késleltetett frissítés, stabilitásra fókuszáló rendszerek számára).

Ezzel a változtatással a szervezetek stratégiai döntést hozhatnak a védelem aktualitása és az üzembiztonság közötti egyensúlyról, ami különösen fontos heterogén vagy kritikus környezetek esetén.

A Microsoft a történtekre reagálva szintén bejelentette egy új, katasztrófaálló rendszerindítási mechanizmus, a Quick Machine Recovery (QMR) bevezetését, amely a Windows 11 24H2-es verziójától lesz elérhető. A szolgáltatás lényege, hogy illesztőprogram- vagy konfigurációs hiba esetén a rendszer automatikusan csökkentett módba vált, majd a Microsoft szervereihez csatlakozva távoli diagnosztikával és javítással képes helyreállítani a működést. Ez az eszköz egy új generációs fault-tolerancia réteget ad a Windows alá, jelentősen csökkentve a hasonló helyzetek manuális beavatkozási igényét.

Összegzés

A 2024. július 19-én bekövetkezett CrowdStrike-incidens világosan demonstrálta, hogy egyetlen, alig 40 kilobájtos konfigurációs frissítés – amennyiben kritikus jogosultsági szinttel és széles körű, automatizált terjesztési mechanizmussal társul – globális működési krízist válthat ki. A hibás channel fájl kernel szinten okozott összeomlást, amely több millió Windows-alapú végpontot tett működésképtelenné, különösen azokban az iparágakban, ahol a valós idejű informatikai rendelkezésre állás létfontosságú feltétel. Repülőterek, kórházak, kormányzati rendszerek és üzleti infrastruktúrák estek ki percek alatt, egy centralizált frissítés hibája miatt.

A technikai ok nem bonyolult: egy hibás memóriakezelési logika egy dinamikusan betöltött, kernel jogosultsággal futó modulban – de az, hogy ez ellenőrizetlenül eljutott milliókhoz, már rendszerszintű kockázatra utal. Az esemény rávilágított arra, hogy a modern végpontvédelmi rendszerek agilitása – gyors frissítés, dinamikus válaszadás – súlyos stabilitási kompromisszumokkal járhat, ha nincs mögötte robusztus, több rétegű tesztelési architektúra. A WHQL-megkerülés, a logikailag hibás validációs pipeline és az automatizált tesztelés téves biztonságérzete együttesen idézték elő a hibát.

Ugyanakkor a CrowdStrike gyors és felelősségteljes válságkezelése, a hibás frissítés visszavonása, a manuális javítási útmutatók kiadása, valamint a teljes technikai transzparencia példaként szolgálhat más szereplők számára. A vállalat teljes átláthatósággal tárta fel a hibák forrását, és konkrét architekturális és eljárásbeli változtatásokat vezetett be annak érdekében, hogy hasonló incidens ne fordulhasson elő.

Az új frissítési modell, a többszintű terjesztési logika és a testreszabható update-csatornák érettebb kockázatmenedzsment-képet mutatnak, mint amit a hiba idején látni lehetett.

A Microsoft válaszlépése – a Quick Machine Recovery mechanizmus bevezetése – szintén azt mutatja, hogy a platformszintű fault-tolerancia és automatizált helyreállítás egyre inkább alapkövetelménnyé válik a globális IT-ökoszisztémában.

Az incidens tanulsága messze túlmutat a CrowdStrike konkrét hibáján: a szoftverfejlesztés és a kiberbiztonság találkozásánál nincsenek mellékes hibák, különösen nem kernel szinten. A digitális világunk törékeny – és ezt nemcsak a rosszindulatú támadások, hanem a jó szándékkal készült, de nem megfelelően ellenőrzött frissítések is képesek bizonyítani. A stratégiai üzenet egyértelmű: a kiberbiztonság nem csak technológiai, hanem folyamat- és felelősségmenedzsment kérdés is – és ezen nem lehet spórolni.

Források

CrowdStrike (2024) External Technical Root Cause Analysis — Channel File 291 Elérhető: https://www.crowdstrike.com/wp-content/uploads/2024/08/Channel-File-291-Incident-Root-Cause-Analysis-08.06.2024.pdf (Letöltve: 2025.05.06)

Sean Michael Kerner (2024) CrowdStrike outage explained: What caused it and what's next Elérhető: https://www.techtarget.com/whatis/feature/Explaining-the-largest-IT-outage-in-history-and-whats-next (Letöltve: 2025.05.06)

Dave's Garage (2024) Dave Plummer explains the CrowdStrike IT Outage - Retired Windows Developer Elérhető: https://www.youtube.com/watch?v=wAzEJxOo1ts (Letöltve: 2025.05.07)

Stanford Report (2024) A computer scientist's take on the CrowdStrike crash Elérhető: https://news.stanford.edu/stories/2024/07/an-expert-s-overview-of-the-crowdstrike-outage (Letöltve: 2025.05.07)

Toby Murray (2024) What is CrowdStrike Falcon and what does it do? Is my computer safe? Elérhető: https://theconversation.com/what-is-crowdstrike-falcon-and-what-does-it-do-is-my-computer-safe-235123 (Letöltve: 2025.05.08)

Esther Linder (2024) What actually happened inside the CrowdStrike update to cause a worldwide IT breakdown? Elérhető: https://www.abc.net.au/news/2024-07-20/what-happened-crowdstrike-global-outage-explainer/104122582 (Letöltve: 2025.05.08)

Cio.com (2024) CrowdStrike failure: What you need to know Elérhető: https://www.cio.com/article/3476789/crowdstrike-failure-what-you-need-to-know.html (Letöltve: 2025.05.08)

Ezo.io (2024) The CrowdStrike Outage: What Happened? Elérhető: https://ezo.io/blog/crowdstrike-outage-and-the-blue-screen-of-death/ (Letöltve: 2025.05.08)

B Shyam Sundar (2024) Technical details of the Windows BSOD disaster due to CrowdStrike Elérhető: https://medium.com/@shyamsundarb/technical-details-of-the-windows-bsod-disaster-due-to-crowdstrike-58de2371c19c (Letöltve: 2025.05.08)

Cwe.mitre.org (2025) CWE-125: Out-of-bounds Read Elérhető: https://cwe.mitre.org/data/definitions/125.html (Letöltve: 2025.05.07)

Zeljka Zorz (2024) CrowdStrike blames buggy testing software for disastrous update Elérhető: https://www.helpnetsecurity.com/2024/07/24/crowdstrike-update-testing/ (Letöltve: 2025.05.08)

Bill Toulas (2024) CrowdStrike: 'Content Validator' bug let faulty update pass checks Elérhető: https://www.bleepingcomputer.com/news/security/crowdstrike-content-validator-bug-let-faulty-update-pass-checks/ (Letöltve: 2025.05.08)


IKE

NEMZETI
KIBERBIZTONSÁGI
INTÉZET

nki.gov.hu

titkarsag@nki.gov.hu

+36 (1) 325 7672

Nemzeti Kibervédelmi Intézet

@ nki.gov.hu

Kibertámadás!
podcast

2025