

ZFO: co ukázalo testování doručenek

Stručný protokol pro veřejnost | Stav k 24. 9. 2026

Testovaná aplikace: Software602 Form Filler 4.81.6.0

U konkrétních pozměněných souborů aplikace hlásila „Obsah je neporušen“, přestože jiné kontroly změnu odhalily. Příčina tohoto rozdílu zatím nebyla určena.

Co se ověřovalo

ZFO je soubor, v němž lze uchovat datovou zprávu nebo doručenkou. Elektronická pečeť umožňuje ověřit, od koho data pocházejí a zda se po zapečetění změnila. Sama ale nezaručuje, že každý údaj je věcně správný. Cílem testů bylo zjistit, co aplikace uživateli zobrazí a jak oznámí zásah do dat.

1. Změněný údaj, ale hlášení o neporušenosti

Ze vzorku „Originál číslo 3 (neporušený)“ vznikla oddělená kopie „Falsum číslo 1 (zásah do dat)“. V ní byl čas události EV0, tedy podání zprávy, posunut o jeden den a předmět výslovně označen jako laboratorní test a falsum. Původní pečeť zůstala zachována; nová platná pečeť k pozměněným údajům nevznikla.

Software602 Form Filler zobrazil změněné údaje a oznámil neporušený obsah. Po další kontrole v aplikaci hlásil i platnou pečeť a důvěryhodný certifikát. Naproti tomu Datovka od CZ.NIC a samostatný ověřovací nástroj OpenSSL zjistily, že podpis neodpovídá obsahu. Nepozměněný výchozí soubor touto kontrolou prošel.

Obdobné nesprávné hlášení neporušenosti bylo pozorováno i u uměle vytvořených testovacích souborů. Důvěra v certifikát a kontrola změn jsou dvě různé věci: důvěryhodný certifikát sám nepotvrzuje, že konkrétní soubor zůstal beze změn.

2. Neexistující datum se zobrazilo

V samostatném testu aplikace zobrazila datum „92.13.1200 v 10:00:00“ bez viditelného upozornění na neplatné datum. Z doslovného vstupu „92.13.1200“ vytvořila text „00..1.92.1 v“. Tyto údaje byly vloženy již před testovacím podpisem. Nešlo tedy o porušení pečeti, ale o zacházení s chybnými vstupními údaji.

Duplicity, tisk a hranice zjištění

3. Dva různé předměty: zobrazil se první

Čtyři umělé vzorky obsahovaly jeden předmět nebo dva rozdílné předměty. U samotné hodnoty ALFA se zobrazila ALFA, u samotné BETA se zobrazila BETA. Při pořadí ALFA, BETA aplikace zobrazila ALFA; při opačném pořadí BETA, ALFA zobrazila BETA. V zachyceném formuláři nebylo upozornění na duplicitu.

Oba předměty byly zahrnuty do testovacího podpisu. Výsledek ukazuje, že v této konkrétní struktuře rozhodlo pořadí údajů. Nedokazuje čtení z nechráněné části souboru ani obejití pečeti. Soulad těchto vzorků se všemi pravidly formátu nebyl potvrzen a výsledek nelze přenášet na jiná pole.

4. Při tisku se objevila další zpráva

Uživatel dodal snímky, na nichž podle jeho popisu po vyvolání tisku přibýlo červené hlášení „Byly provedeny změny“. Současně zůstalo „Obsah je neporušen“, a to i v podrobnostech zabezpečení. Snímky tak zachycují pro běžného čtenáře nejasná souběžná sdělení.

Doplněná kontrola ukázala stejné hlášení i u neporušeného originálu a nového umělého vzorku. Soubory na disku zůstaly beze změny a jejich podpisy prošly samostatnou kontrolou. Hlášení při tisku tedy samo nerozlišuje porušení pečeti; může souviset se změnou pracovního formuláře.

Co se neprovedlo a co nelze tvrdit

Pokus s rozdílnými hodnotami v chráněné a nechráněné části souboru nebyl proveden. Asistent jej v dřívějším kontextu žádosti o skryté pozměnění odmítl; pro tento pokus nevznikl vzorek ani výsledek. Odmítnutí nic nedokazuje o možnosti takové chyby. Test dvou podepsaných předmětů tento pokus nenahrazuje.

Hlavní test skutečné doručky proběhl v odděleném laboratorním prostředí Sandboxie. Jeho opakování na čisté instalaci mimo toto prostředí zatím není doloženo. Neproběhl úplný audit programu ani test všech jeho verzí. Nebylo prokázáno prolomení pečeti, převzetí aplikace nebo napadení systému datových schránek.

Podklady a význam pro veřejnost

Text zkracuje souhrnný protokol z 24. 9. 2026, sestavený z uložených výsledků a snímků s pomocí asistenta Codex. Veřejný balíček obsahuje 12 umělých ZFO, snímky a kontrolní otisky pro identifikaci souborů. Skutečné doručky a snímky s osobními údaji nejsou zveřejněny. Nejde o znalecký posudek.

Samotné ujištění v okně aplikace v popsáných testech nestačilo. Pro veřejnou diskusi je podstatné nezávislé zopakování a vysvětlení, co jednotlivá hlášení skutečně ověřují.