CTI Riport

NETLOCK gyökértanúsítvány megbízhatóságának várható megszűnéséről a Google platformjain

2025. június 6.

Tartalom

Összegzés

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet rendszeresen végez elemzéseket a hozzá beérkező, harmadik féltől származó információk, valamint saját kutatásai alapján. Az alábbi riport során a „NetLock Arany (Class Gold) Főtanúsítvány” Google platformjain való várható megbízhatatlanná tételéről szól.

2025. augusztus 1-jétől a Google megszünteti a bizalmat a NETLOCK egyik gyökértanúsítványa iránt. Ez jelentős kiberbiztonsági és üzleti kockázatot jelenthet azon szervezetek számára, amelyek tanúsítványa erre az aláíróra épül. Bár a titkosított adatátvitel technikailag továbbra is működhet, a 2025. július 31. után ezen tanúsítványhitelesítő (CA) által kiállított tanúsítványokat a böngészők és kliensek nem tekintik megbízhatónak, így a felhasználóknál biztonsági figyelmeztetések jelenhetnek meg. Ez jelentős reputációs kárt, valamint üzemeltetési problémákat okozhat a szolgáltatásban.

A Google nem részletezte döntésének pontos okait, de a Mozilla közösség által végzett vizsgálatok alapján valószínűsíthető, hogy a NETLOCK tanúsítványkiadási gyakorlatával, átláthatóságával és a szabályozási előírásoknak való megfeleléssel kapcsolatos problémák vezettek a bizalomvesztéshez. Az Apple rendszerein a kérdéses gyökértanúsítvány már 2024. július 30. óta nem számít megbízhatónak, így a mostani bejelentés egy tágabb iparági trendbe illeszkedik.

A tanúsítványhitelesítők megbízhatóságának elvesztése – még kisebb, adminisztratív jellegű hibák következtében is – a nyilvános kulcsú infrastruktúra (PKI) természetéből fakadóan elkerülhetetlen. Ez nem a rendszer gyengesége, hanem épp annak egyik legfontosabb biztonsági erénye. A szigorú megfelelési elvárások biztosítják a digitális tanúsítványokon alapuló ökoszisztéma integritását. Jelen riport célja, hogy feltérképezze a döntés lehetséges hatásait, az érintett szervezetek kockázatait, valamint a válaszlépéseket a kialakult helyzet kezelésére.

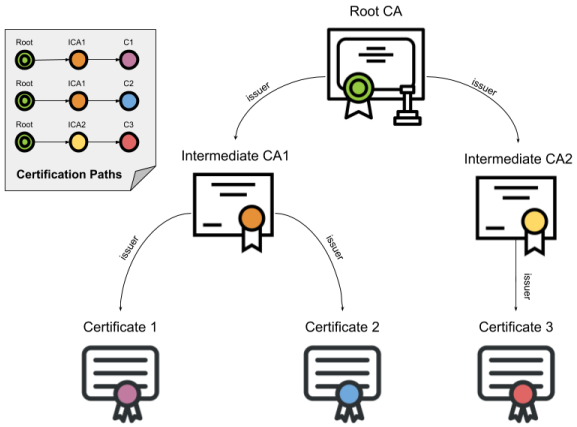
Az érintett gyökértanúsítvány

A gyökértanúsítvány megbízhatóságának elvesztése nem technikai sebezhetőséget, hanem bizalmi problémát jelent, ami a nyilvános kulcsú infrastruktúra (PKI) ökoszisztéma egyik legérzékenyebb pontja. Mivel a NETLOCK által kibocsátott tanúsítványok nagy része e gyökér alatt található, a változás széleskörűen érintheti Magyarország köz- és magánszektor webes szolgáltatásait.

A Google a saját platformjain augusztus 1-től a NetLock Arany (Class Gold) Főtanúsítványt[1] nem megbízhatónak fogja tekinteni. A Root CA-ról az alábbi információk állnak rendelkezésünkre:

- Kibocsájtó tulajdonos (CN): NetLock Arany (Class Gold) Főtanúsítvány
- Kibocsájtó szervezet neve: NetLock Kft.
- Érvényes: 2028-12-06T 15:08:21GMT
- Sorozatszám: 80544274841616

Ez a tanúsítvány egy gyökértanúsítvány (Root CA), amely a NETLOCK nyilvános kulcsú infrastruktúrájának alapját képezi. A NETLOCK ezen keresztül közbenső tanúsítványokat bocsát ki, amelyek pedig végfelhasználói tanúsítványokat írnak alá.



1. ábra: Tanúsítvány validálás folyamata.
Forrás: ssl.com

1 https://crt.sh/?q=6c61dac3a2def031506be036d2a6fe401994fbd13df9c8d466599274c446ec98

A tanúsítványlánc-ellenőrzés során a böngészők és operációs rendszerek először a végfelhasználói tanúsítványt, majd a közbenső tanúsítványokat, végül pedig az egész lánc végén található gyökértanúsítványt ellenőrzik. Amennyiben a lánc nem vezet megbízható (trusted) gyökértanúsítványhoz, a böngésző biztonsági figyelmeztetést jelenít meg, és a kapcsolatot nem tekinti megbízhatónak.

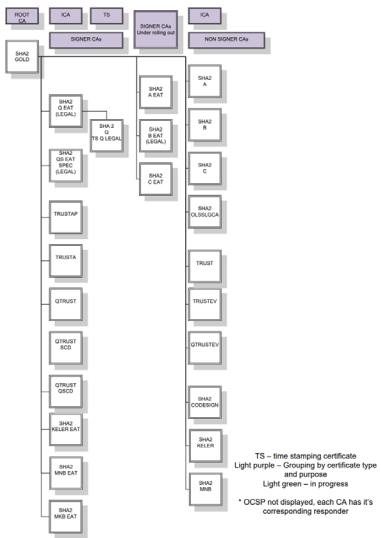
A Google döntése értelmében 2025. augusztus 1-jétől a NETLOCK egyik root tanúsítványa elveszíti megbízhatóságát a Chrome és Android platformokon.

Ennek következtében az ehhez a gyökérhez tartozó tanúsítványláncokat, amelyekhez a legkorábbi Signed Certificate Timestamp (SCT) 2025. július 31. 23:59:59 UTC után keletkezett, nem fogják megbízhatónak tekinteni.

Ez minden ilyen láncra épülő közbenső és végfelhasználói tanúsítványt érinthet, és biztonsági figyelmeztetéseket okozhat a felhasználói oldalon.

Az érintett tanúsítványok között található minden olyan tanúsítvány, amelyet olyan közbenső CA írt alá, amely maga is a fent említett Root CA alatt szerepel. Ezekre az Issuer Organization Name mezőben a következők utalnak:

- NETLOCK Kft.
- NETLOCK Ltd.



2. ábra: A NETLOCK CA hierarhiája.
Forrás: https://www.netlock.hu/docs/dokumentumok/NETLOCK_ca_hierarchy.pdf
Az érintett root CA „SHA2 GOLD” néven látható.

A bizalomvesztés lehetséges okai

A Google jelenleg nem közölte nyilvánosan a konkrét indoklást a bizalommegvonás mögött. Ennek következtében a pontos technikai vagy működési ok ismeretlen.

Ugyanakkor az ügy nem elszigetelt, és egy másik fontos szereplő – a Mozilla – párhuzamos vizsgálatokat folytat a NETLOCK tanúsítványkezelési gyakorlataival kapcsolatban[2] [3] [4]. A Mozilla hibajegyeiben és vizsgálati anyagaiban több probléma is dokumentálásra került, köztük a közbenső tanúsítványok késedelmes bejelentése, hiányos átláthatóság, valamint az incidensek dokumentálásának elmulasztása.

Míg a Mozilla vizsgálatai nem feltétlenül állnak közvetlen kapcsolatban a Google döntésével, technikai szempontból fontos háttérinformációt nyújtanak az érintett CA működéséről.

Lejárt tanúsítvány szolgáltatása tesztoldalon

A valid.ev.tanusitvany.hu című, a CCADB adatbázisban „Valid Test Website”-ként regisztrált NETLOCK-tesztoldal 2025. április 5-én egy lejárt EV TLS tanúsítványt kezdett kiszolgálni. A tanúsítvány a NetLock Arany (Class Gold) gyökértanúsítványhoz kapcsolódott.

Valid Test Website

Egy szabványos iparági követelmény a hitelesítésszolgáltatók (CA-k) számára, amely szerint a CA-nak nyilvánosan elérhető tesztcélú HTTPS-weboldalt kell fenntartania, amelyen érvényes TLS-tanúsítványt szolgáltat.

[2] https://bugzilla.mozilla.org/show_bug.cgi?id=1962426
[3] https://bugzilla.mozilla.org/show_bug.cgi?id=1904041
[4] https://bugzilla.mozilla.org/show_bug.cgi?id=1957474

Ez megsértette a CA/Browser Forum Baseline Requirements 2.2 pontját[5], amely előírja, hogy a "Valid" tesztoldal mindig érvényes, nem lejárt és nem visszavont tanúsítványt kell hogy szolgáltasson.

Common CA Database (CCADB)

Egy olyan adatbázis, amely információkat tartalmaz azokról a tanúsítványkiadókról (CA-k), amelyek gyökér- és közbenső tanúsítványai szerepelnek több gyökértár-üzemeltető termékeiben és szolgáltatásaiban. Ezek a gyökértár-üzemeltetők a CCADB-t használják a saját gyökértáraikban szereplő tanúsítványkiadók.

A tanúsítvány megújítása feltehetően azért maradt el, mert a szervezet épp automatikus tanúsítványkezelésre tért át, mely közben a monitoring rendszer nem volt megfelelően felkonfigurálva, ami következtében a szervezet nem kapott riasztást a lejárt tanúsítványról, az automatizálás miatti átállás következtében pedig a manuális megújítás nem történt meg.

A hiba során csak egy tanúsítvány volt érintett, a reagálási idő pedig kifejezetten lassúnak volt mondható, mivel a tanúsítvány 2025-04-05 07:46-kor járt le, és csak 2025-04-28 16:12-kor cserélték.

Közbenső tanúsítványok bejelentésének hiánya

A NETLOCK 2024 májusában négy új közbenső tanúsítványt (Intermediate CA) bocsátott ki, amelyek egy új tanúsítványlánc részét képezik. Ezeket a tanúsítványokat a Common CA Database (CCADB) nevű nyilvános adatbázisba kell bejelenteni, a CCADB Policy v1.3.1 – 5.1.2.2 szakasza alapján, legkésőbb a kibocsátást követő 7 napon belül, ami elmulasztásra került.

5 https://cabforum.org/working-groups/server/baseline-requirements/requirements/#22-publication-of-information

Az érintett CERT-ek SHA-256 azonosítói az alábbiak:

- 001279B949DD8670F1AE6DA407913B726F61AEF78A2FF19C2DA39522B31DC0C7
- F37E7AD92ECEA12F307501C126B3E2D6DE2C7417D3E1B72D26069C1370E78894
- D0EB908401F33242602634AFD51991536B3AD7AA901586FDEB4955FE51B0E419
- 17771F6947FA3472786D3A44B5ADE2AACBA9ADA203BA31EBD4BD8CEBAFCE494A

A NETLOCK kivizsgálta az esetet, és megállapította, hogy adminisztrációs hiba történt. A közbenső tanúsítványok dokumentációja és benyújtása során felcserélték a keresztaláírt és a nem keresztaláírt közbenső CA-t.

Keresztaláírt gyökértanúsítvány

A keresztaláírt gyökértanúsítvány olyan digitális tanúsítvány, amelyet egy tanúsítványkiadó hatóság (CA) bocsát ki egy másik CA gyökértanúsítványának megerősítéseként. Ez a mechanizmus a nyilvános kulcsú infrastruktúrában (PKI) lehetővé teszi a bizalom kiterjesztését különböző hitelesítésszolgáltatók között, és gyakran alkalmazzák arra, hogy áthidalják az eltérő root store-ok közötti bizalmi különbségeket.

Így a valóban szükséges keresztaláírt közbenső tanúsítványok helyett olyan tanúsítványokat jelentettek be a CCADB-ben, amelyekre nem lett volna szükség. A tanúsítványok nagyon hasonlóak voltak (azonos tárgynév és nyilvános kulcs), illetve mivel nem volt ellenőrzőlista a regisztráció előtti ellenőrzéshez, a hibát nem vették észre időben (az Issuer mező ellenőrzése segíthetett volna ezt megelőzni). A hiba kijavítása után minden tanúsítvány megfelelően szerepel a nyilvántartásban.

Heti jelentések elmaradása

2025-ben a NETLOCK több, nyitott incidensjegy esetében elmulasztotta a heti frissítések határidőben történő biztosítását, megsértve ezzel a CCADB Incident Reporting Guidelines[6] előírásait. Az incidens nem érintett tanúsítványkibocsátást, kizárólag az incidenskezelésre és kommunikációra vonatkozó eljárásokra terjedt ki.

A késedelmes válaszadás hátterében egy új, többlépcsős és összetett belső folyamat bevezetése állt, amelyet a munkatársak nem teljeskörűen sajátítottak el. A munkatársak képzése túlnyomórészt részfolyamatokra koncentrált, és nem biztosította a rendszer egészének átlátását. Emellett a belső jóváhagyási láncok túl lassúak és bürokratikusak voltak, így a kötelező heti kommunikációk nem készültek el időben.

A NETLOCK a kivizsgálást követően átalakította a képzési anyagokat, egyszerűsítette az eljárásokat, valamint újra oktatta a munkatársait a teljes folyamat átláthatóbbá tétele érdekében.

Összegzés

A NETLOCK főtanúsítványa iránti bizalom megingását vélhetően a felsorolt három dokumentált hiányosság, vagy azokhoz hasonló esemény idézte elő. Bár ezek önmagukban nem tűnnek súlyosnak, a nyilvános kulcsú infrastruktúra (PKI) sajátosságából fakadóan már kisebb adminisztratív vagy működési hibák is elegendőek lehetnek ahhoz, hogy egy tanúsítványhitelesítő elveszítse megbízhatóságát. Ez a szigorúság ugyanakkor nem hiba, hanem a rendszer egyik alapvető erénye: éppen ez biztosítja a PKI ökoszisztéma magas szintű biztonságát és integritását.

[6] https://www.ccadb.org/cas/incident-report

Érintetti vizsgálat

A rendelkezésre álló források alapján megállapítható, hogy a jövőben megújítandó, ezért potenciálisan érintett tanúsítványok túlnyomó többsége Magyarországon működő szervezetekhez köthető. Ez összhangban áll azzal, hogy a NETLOCK Kft. elsősorban hazai szolgáltatóként van jelen a tanúsítványkiadás piacán, és külföldi jelenléte marginális.

- Magyarországi érintettek száma[7]: 1 581 darab tanúsítvány
- Ebből kormányzati szereplők (gov.hu tartomány): 166 darab
- Nemzetközi érintettség: 135 darab tanúsítvány

A földrajzi koncentráció következtében a bizalmi státusz megszűnésének hatása elsősorban a magyarországi közigazgatásra, közszolgáltatásokra és hazai vállalati infrastruktúrákra gyakorolhat közvetlen hatást. Nemzetközi szinten az incidens hatása várhatóan korlátozott marad.

[7] A riport írásakor, a szám napról-napra változhat

Az NBSZ-NKI által javasolt intézkedések

Tanúsítványcsere

Amennyiben az Ön szolgáltatása olyan TLS/SSL tanúsítványt használ, amelyet a NETLOCK Kft. vagy NETLOCK Ltd. bocsátott ki, és a tanúsítványt 2025. július 31. után kell megújítani, javasoljuk, hogy térjen át egy másik, nemzetközileg elismert tanúsítványkiadóra (CA).

Amennyiben belső vállalati hálózatban megbízhatónak kívánja tekinteni a tanúsítványokat

Amennyiben a NETLOCK által kibocsátott, a Google bizalmi köréből kivezetésre kerülő tanúsítványokat kizárólag belső vállalati hálózaton használja (pl. belső webes alkalmazásokhoz vagy rendszerekhez), és továbbra is megbízhatónak kívánja tekinteni azokat a Chrome böngészőben, úgy erre továbbra is lehetősége van. A Chrome 127-es verziójától kezdődően a vállalatok felülírhatják a Chrome Root Store által alkalmazott bizalmi korlátozásokat azáltal, hogy az érintett root tanúsítványt helyileg megbízható gyökértanúsítványként telepítik arra a rendszerre, amelyen a Chrome fut (például a Windows Tanúsítványtároló „Trusted Root Certification Authorities” részébe). Ezáltal a belső hálózaton továbbra is biztosítható a tanúsítványok bizalmi státusza, függetlenül a Google alapértelmezett beállításaitól.

Kérjük, amennyiben a vizsgálattal összefüggően további kérése merül fel, vagy hiányosságot azonosított, értesítse intézetünket a cyberthreat@nki.gov.hu, vagy CSIRT@nki.gov.hu címen.

Nemzetbiztonsági Szakszolgálat
Nemzeti Kibervédelmi Intézet