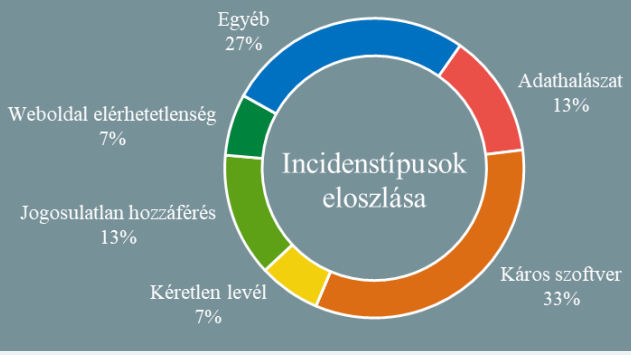
NEMZETI KIBERVÉDELMI INTÉZET

Nemzetközi IT-biztonsági sajtószemle

2021. 37. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2021.09.10. - 2021.09.16.



Kövessen minket megújult weboldalunkon, ahol friss IT biztonsági hírek kerülnek publikálásra!

SSID Stripping: a hamis hálózatokkal való megtévesztés

(securityweek.com)

Egy új módszert azonosítottak a kutatók, amellyel a támadók elérhetik, hogy úgy csatlakozzanak az áldozat vezeték nélküli hozzáférési pontjához (AP), hogy arról az érintett ne szerezzen tudomást. Az SSID Strippingnek nevezett módszert 2021. szeptember 13-án hozta nyilvánosságra a vezeték nélküli biztonságra szakosodott AirEye, amely a Technion (Izraeli Technológiai Intézet) kutatóival együttműködve fedezte fel a hibát. A biztonsági rés a Windows, macOS, Ubuntu, Android és iOS rendszert futtató eszközöket érinti. **Bővebben...**

Adatvédelmi újítással érkezik az Android 12 béta verziója

(securityaffairs.co)

A Google bemutatta legújabb szolgáltatáscsomagját, a Private Compute Sevices-t, amelynek célja, hogy javítsák a felhasználók magánéletének védelmét. Az Android 12 béta verziójához már hozzáadásra is került a Private Compute Core, ami egy nyílt forráskódú, az operációs rendszertől és alkalmazásoktól elszigetelt biztonságos környezet. A terek szerint a jövőben minden új Android verzióval további adatvédelmi funkciókkal kerül majd bővítésre az új szolgáltatás. **Bővebben...**

IT biztonsági Tanács

Az NBSZ NKI weboldalán a Microsoft jelszómentes bejelentkezéséről olvashatnak bővebb információkat.

Titkosított biztonsági mentésekkel rukkolt elő a WhatsApp

(thehackernews.com)

A WhatsApp bejelentette, hogy rövidesen támogatni fogja, hogy a chatüzenetekről végponttól-végpontig titkosított biztonsági mentést lehessen tárolni a felhőben. A funkció a következő hetekben lesz elérhető a felhasználók számára, amelynek következtében az Android felhasználók a Google Drive-ba, az Apple felhasználók pedig az iCloudba menthetik majd titkosítva az alkalmazáson belüli üzeneteiket és fényképeiket. Mindez feltehetően csak az elsődleges, a szolgáltatáshoz társított eszközökön lesz elérhető, így a funkció nem terjed ki például a számítógépes platformokra. **Bővebben...**

Kritikus hiba a Pac-Resolver NPM csomagban

(securityaffairs.co)

A szakértők kritikus hibát (CVE-2021-23406) találtak a 'Pac-Resolver' NPM csomagban, amelyet hetente több millióan töltenek le. A sebezhetőséget kihasználva a támadók rosszindulatú kódot futtathatnak a Node.js alkalmazásokon belül. A hiba a Pac-Resolver 5.0.0 előtti verzióit érinti, és 8,1-es CVSS pontszámot kapott. Egy proxy auto-config (PAC) fájl határozza meg, hogy a webböngészők és más kliensalkalmazások hogyan tudják automatikusan kiválasztani a megfelelő proxyt (hozzáférési módszert) egy adott URL lekérdezéséhez. **Bővebben...**

Chrome felhasználók figyelem, ideje frissíteni!

(thehackernews.com)

A Google hétfőn biztonsági frissítést adott ki, amelyben a Chrome böngésző 11 db – ebből a támadók által kettő aktívan kihasznált – zero-day sérülékenysége került javításra. A **CVE-2021-30632** és **CVE-2021-30633** néven bejegyzett sebezhetőségek memóriakezelési problémákból adódnak, amelyek közül az egyiket a V8-as JavaScript motor komponensben, míg a másikat az indexelt DP API-ban alkalmaznak. A Google tisztában van a sérülékenységek aktív kihasználásával, azonban nem osztott meg részleteket a támadások elkövetőiről, jellegéről és célcsoportjáról. **Bővebben...**