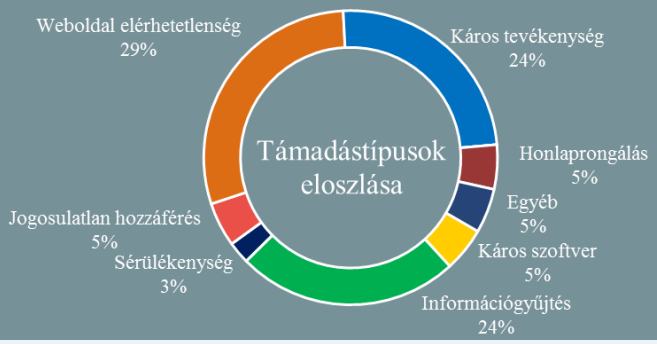
NEMZETI KIBERVÉDELMI INTÉZET

Nemzetközi IT-biztonsági sajtószemle

2020. 41. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2020.10.02. - 2020.10.08.



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

Frissítsen: kritikus sérülékenységeket javított a QNAP

(bleepingcomputer.com)

A QNAP nemrég adott ki tájékoztatót egy sérülékeny NAS eszközeit célzó zsarolóvírusról (AgeLocker), most pedig két kritikus kockázati besorolású biztonsági résről (CVE-2020-2506, CVE-2020-2507) számolt be, amelyek lehetővé tehetik egy támadó számára, hogy távolról átvegye az irányítást a sérülékeny eszköz felett. A biztonsági hiba a QNAP NAS-ok beépített **Helpdesk alkalmazását** érinti, amivel a rendszer gazdája felveheti a kapcsolatot a QNAP support csapatával hiba esetén. Az alkalmazás rendelkezik egy távsegítség funkcióval, így – ha a hibaelhárítás során indokolt – a support képes az ügyfél jogosultsági szintjén távolról menedzselni az eszközt. **Bővebben...**

Telegram és a Threema alkalmazásoknak adja ki magát egy új androidos kémprogram

(thehackernews.com)

Telegram és Threema üzenetküldő alkalmazásoknak álcázza magát az Android/SpyC23 spyware, amelyet a 2017 óta ismert, közel-keleti APT-C-23 csoporthoz kötnek. (2020 elején a Check Point Research foglalkozott az APT-C-23 tevékenységével, amikor a Hamász tagjai magukat tizenéves lányoknak kiadva több közösségi portálon – Facebook, Instagram és Telegram – profilokat regisztráltak, hogy rosszindulatú alkalmazások telepítésére vegyenek rá izraeli katonákat.) **Bővebben...**

IT biztonsági Tanács

Az NBSZ NKI weboldalán hasznos információkat olvashat az iOS 14 új adatvédelmi funkcióiról.

Figyelem: a HP Device Managert érintő kritikus sérülékenységek némelyikére még nincs javítás, de workaround elérhető

(securityaffairs.co)

A HP három kritikus kockázati besorolású biztonsági hibáról (CVE-2020-6925, CVE-2020-6926, CVE-2020-6927) adott ki tájékoztatót a HP vékonykliensek távmenedzselését lehetővé tévő HP Device Manager kapcsán, amelyek kihasználásával egy támadó átveheti az irányítást az érintett, Windowst futtató HP vékonykliensek felett. A CVE-2020-6925 és CVE-2020-6926 azonosítójú hibákra a gyártó még nem adott ki javítást, a CVE-2020-6927 számú sérülékenység azonban javítva lett a **Device Manager 5.0.4**-es verziójában. **Bővebben...**

Tenda routerek veszélyben: új IoT botnet a láthatáron

(zdnet.com)

Távoli hozzáférésű trójai (Remote Access Trojan – RAT) funkciókkal is bír az az új kártevő, ami sérülékeny Tenda routerekből épít robothálózatot. A **Ttint** névre keresztelt botnetet a Netlab fedezte fel, amely a kínai tech óriás Qihoo 360 hálózatbiztonsági divíziója. A cég jelentése szerint a botnet nem csupán a standard botnet funkcióval – DDoS képesség – rendelkezik, hanem 12 különböző káros tevékenységet tesz lehetővé a támadó számára. Például a DNS beállítások módosításával káros oldalakra irányíthatja a támadott eszköz felhasználóját, proxynak használhatja az eszközt saját forgalmának routolására, vagy épp tetszőleges kódot futtathat. **Bővebben...**

Biztonsági hibákat találtak népszerű antivírus szoftverekben

(securityaffairs.co)

A CyberArk Labs biztonsági kutatói olyan sérülékenységeket azonosítottak népszerű antivírus szoftverekben, amelyeket a támadók felhasználhatnak arra, hogy emelt szintű jogosultságot nyerjenek a megcélzott rendszeren. Többek közt a Kaspersky, McAfee, Symantec, Fortinet, Check Point, Trend Micro, Avira, és Microsoft védelmi termékei is sérülékenynek bizonyultak. A probléma sok esetben a *C:\ProgramData könyvtár* hozzáférés-kezeléséből fakadt. **Bővebben...**