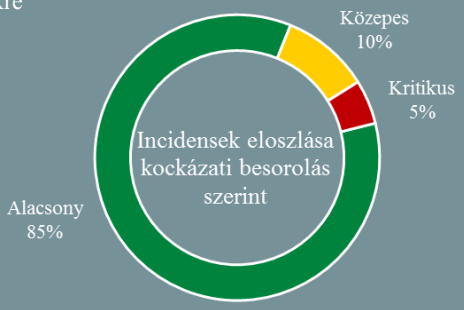
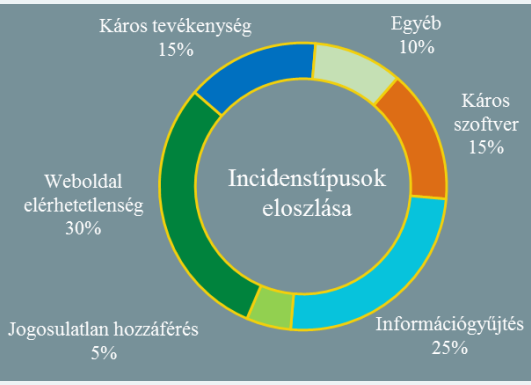
NEMZETI KIBERVÉDELMI INTÉZET

Nemzetközi IT-biztonsági sajtószemle

2021. 50. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2021.12.10. - 2021.12.16.





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

Webszerver adminok figyelem: aktívan támadják a Log4j sérülékenységét!

(bleepingcomputer.com)

Log4Shell vagy LogJam néven is hivatkoznak a Log4j naplózó keretrendszer kritikus sérülékenységére (**CVE-2021-44228**), amely jogosulatlan távoli kódfuttatást tesz lehetővé a sérülékeny rendszereken. A Log4j egy nyílt forrású, Java-alapú programkönyvtár, amelyet több millió Java alkalmazás használ hibaüzenetek naplózására. A sérülékenység rendkívül egyszerűen kihasználható, csupán azáltal, hogy a támadó egy speciális karakterláncot állít be User Agentként a szervernek küldött HTTP fejlécben. A sérülékenységről friss információkat az NBSZ NKI weboldalán itt találhat. **Bővebben...**

Kritikus biztonsági réseket foltoz be az Apple új frissítése!

(thehackernews.com)

A Tianfu Cupon elnevezésű Kínában megrendezett hackerversenyen, több, az Apple operációs rendszereiben található sérülékenységet tártak fel. Ehhez kötődően az Apple biztonsági frissítést adott ki iOS, macOS, tvOS, és a watchOS rendszerű eszközeihez. A hibajavítás többek közt a CVE-2021-30955 számú sérülékenységet is befoltozza, amelynek kihasználásával a támadók egy rosszindulatú alkalmazás segítségével tetszőleges kódot futtathatnak kernel szintű jogosultsággal. **Bővebben...**

IT biztonsági Tanács

Az NBSZ NKI weboldalán szervezeti vezetők és IT üzemeltetők hasznos információkat olvashatnak arról, hogy szervezetük **miért** és **hogyan** erősítse kibervédelmét az ünnepi időszak alatt.

Ilyen típusú TP-Link routert használ? Frissítsen!

(fortinet.com)

A TP-Link TL-WR840N (V5) típusú hálózati útválasztót egy olyan sérülékenység (CVE-2021-41653) sújtja, amely lehetőséget ad a támadó számára, hogy átvegye az irányítást a sérülékeny eszköz felett. A Fortinet jelzése szerint támadók a sérülékenységet aktívan ki is használják, hogy a fertőzött eszközöket egy Mirai-alapú robothálózatba (MANGA, vagy más néven Dark) kapcsolják, és azokat elosztott szolgáltatásmegtagadás (DDoS) támadásokhoz használják fel. A sérülékenység csak a termék **5-ös hardververzióját érinti**. TP-Link router tulajok eszközük hátoldalán tudják ellenőrizni a router verzióját, ehhez magyar nyelvű gyártói segítség itt található. **Bővebben...**

A Dell illesztőprogram javítás még mindig lehetővé teszi a Windows Kernel elleni támadásokat

(bleepingcomputer.com)

2021 májusában nyilvánosságra hoztak és javítottak öt különböző, együttesen CVE-2021-21551 számon nyomon követhető sebezhetőséget, amelyek Dell számítógépek illesztőprogramjait érintik, és mintegy 12 évig voltak kihasználhatóak. 2021 decemberében kiderült, hogy nem volt elég átfogó a biztonsági frissítés, és továbbra is kihasználhatók maradtak a hibák, amelyek ún. BYOVD (Bring Your Own Vulnerable Driver) támadások során aknázhatók ki. Ez egy olyan támadási technika, amelyben a támadók egy legitim, de sebezhető illesztőprogramot telepítenek a célgépre, majd ezt használják ki a jogosultságok növelésére vagy kód futtatására. **Bővebben...**

Ismeretlen AirTag eszközöket észlelő androidos appot adott ki az Apple

(therecord.media)

Hétfőtől elérhető az Androidos készülékeket használók számára a Google Play áruházban az Apple által készített Tracker Detect névre keresztelt alkalmazás, amely az eszköz közelében található ismeretlen – így potenciálisan ártó szándékkal használt ─ AirTagek észlelésére szolgál. **Bővebben...**