NEMZETBIZTONSÁGI SZAKSZOLGÁLAT 1996

NEMZETI KIBERVÉDELMI INTÉZET

HÍRLEVÉL

Nemzetközi
IT-biztonsági sajtószemle
2023. 51. hét

HÍREK

- RCE sebezhetőségeket találtak két népszerű WordPress bővítményben
- A billentyűzet gépelésének hangja elárulhatja a jelszavát
- Az orosz APT28 hackerei 13 nemzetet vettek célba
- RCE sebezhetőséget javítottak a WordPress 6.4.2-es verziójában
- Mi a teendő, ha kéretlen egyszer használatos jelszó érkezik?

SÉRÜLÉKENYSÉGEK

- Riasztás Microsoft termékeket érintő sérülékenységekről
- Tájékoztatás Adobe szoftverek sérülékenységeiről

IT BIZTONSÁGI TIPP

- Aggályokat vethet fel egy híres alkalmazás a Facebookon

STATISZTIKAI ADATOK

- Incidensek eloszlása típus és kockázati besorolás szerint
- Események eloszlása csapdatípusok alapján
- Támadott port szerinti eloszlás

KONTAKT

edt@nki.gov.hu

PGP kulcs

FBC3 88A2 E465 BF51
AD58 A2D0 E9DD E078
ABD3 E75D

NEWS

IT biztonsági
HÍREK

A billentyűzet gépelésének hangja elárulhatja a jelszavát
(malwarebytes.com)

A Durham University, a University of Surrey és a Royal Holloway University of London által kifejlesztett technika a jelszó kitalálásának még pontosabb módját kínálja a billentyűzeten történő gépelés hangjának meghallgatásával. **Bővebben...**

Az orosz APT28 hackerei 13 nemzetet vettek célba
(securityaffairs.com)

A megfigyelések szerint az APT28 néven ismert orosz nemzetállami szereplő a folyamatban lévő Izrael-Hamász háborúval kapcsolatos csalikat használt fel a *HeadLace* nevű backdoor kihasználásának megkönnyítésére. **Bővebben...**

RCE sebezhetőséget javítottak a WordPress 6.4.2-es verziójában
(securityaffairs.com)

Javítottak egy biztonsági sebezhetőséget a WordPress 6.4.2-es verziójában, ami által egy másik hibával összekapcsolva távoli kódvégrehajtás válik lehetővé. A WordPress hivatalos útmutatója szerint a hiba önmagában közvetlenül nem kihasználható, viszont egy másik sérülékenységgel együtt már kritikus szintű, különösen multisite telepítések esetén. **Bővebben...**

Mi a teendő, ha kéretlen egyszer használatos jelszó érkezik?
(bleepingcomputer.com)

Aggodalomra adhat okot, ha váratlanul érkezik hozzánk egy egyszer használatos jelszó *(OTP: One-time passcode)*, hiszen felmerülhet a gyanú, hogy ellopták a belépési azonosítóinkat. **Bővebben...**

IT biztonsági
TIPP

RCE sebezhetőségeket találtak két népszerű WordPress bővítményben
(securityweek.com)

Kritikus távoli kódfuttatást (RCE) eredményező sebezhetőségeket találtak a Backup Migration és az Elementor nevű WordPress bővítményekben. **Bővebben...**

IT biztonsági Tipp

Az NBSZ NKI weboldalán egy aktuális Facebook alkalmazás, a My Puzzles veszélyeiről tudhatunk meg többet.

Aktuális tartalmak

Aggályokat vethet fel egy híres alkalmazás a Facebookon

Újabb szórakoztató alkalmazás jelent meg a Facebookon, amelyben a mesterséges intelligencia segítségével különböző módokon alakíthatjuk át a fényképeinket.
A virálissá vált alkalmazás nem más, mint a "**My Puzzles**", amely sok ember számára ismerős lehet, hisz nemtől, kortól függetlenül rengeteg ember osztja meg az ezzel készített fotóit üzenőfalán. Azonban érdemes körültekintőnek lenni, mivel ennek használata számos aggasztó tényezőt vet fel a játék biztonságosságával kapcsolatban.

Elolvasom

További érdekességekért és IT biztonsággal kapcsolatos tartalmakért látogasson el közösségi oldalainkra!

Nemzeti Kibervédelmi Intézet

@nki.gov.hu

TÁJÉKOZTATÓK, SÉRÜLÉKENYSÉGEK, RIASZTÁSOK

Riasztás Microsoft termékeket érintő sérülékenységekről

A Microsoft 2023. december havi biztonsági csomagjában összesen 34 különböző biztonsági hibát és egy korábban nyilvánosságra hozott AMD CPU sebezhetőséget javított, köztük 4 kritikus kockázati besorolásút, amelyek kihasználása távoli kódfuttatást, szolgáltatásmegtagadást és jogosultság kiterjesztést tesz lehetővé a sérülékeny rendszeren.

- **CVE-2023-36019 (Microsoft Power Platform Connector Spoofing Vulnerability)**
- **CVE-2023-35630 (Internet Connection Sharing (ICS) Remote Code Execution Vulnerability)**
- **CVE-2023-35641 (Internet Connection Sharing (ICS) Remote Code Execution Vulnerability)**
- **CVE-2023-35628 (Windows MSHTML Platform Remote Code Execution Vulnerability)**

Bővebben...

Tájékoztatás Adobe szoftverek sérülékenységeiről

Összesen **214 különálló CVE számmal rendelkező sérülékenység** került javításra, ezek közül – a gyártói besorolás szerint – **13 kritikus** és **195 db magas** kockázati besorolású.

Az NBSZ NKI a biztonsági frissítések haladéktalan telepítését javasolja, amelyek elérhetőek az automatikus frissítésen keresztül, valamint manuálisan is letölthetők a gyártói honlapokról.

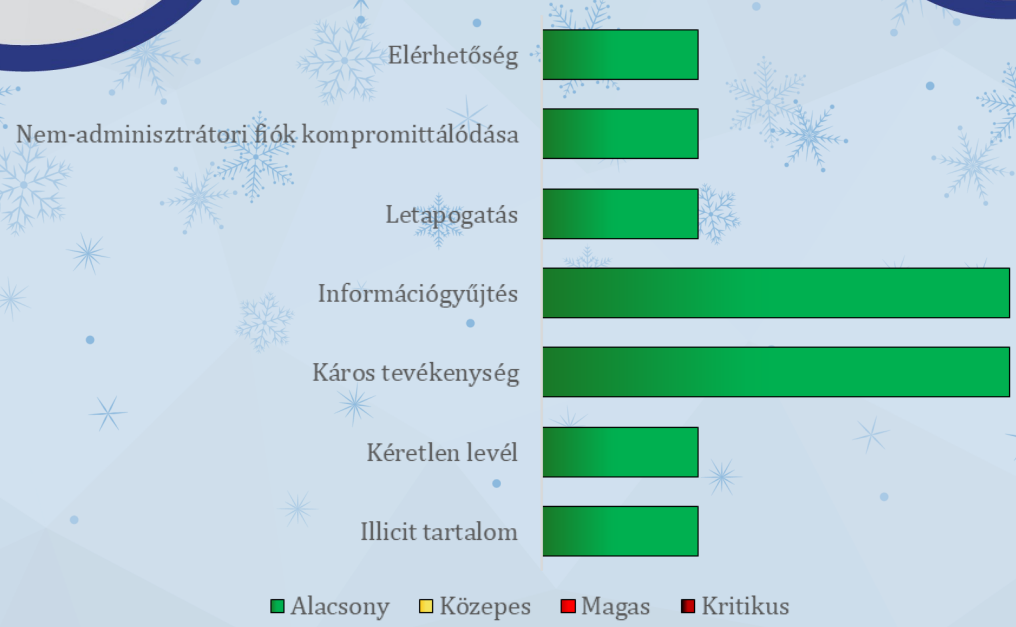
Bővebben...

Statisztikai adatok

2023.12.15.-2023.12.21.

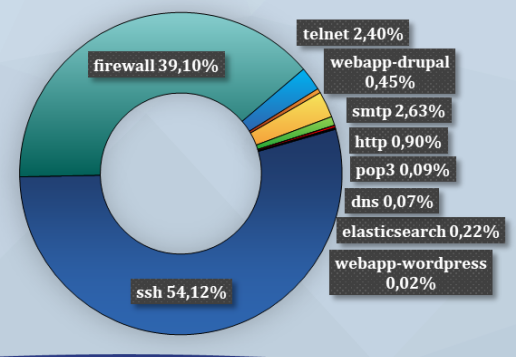
Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok:

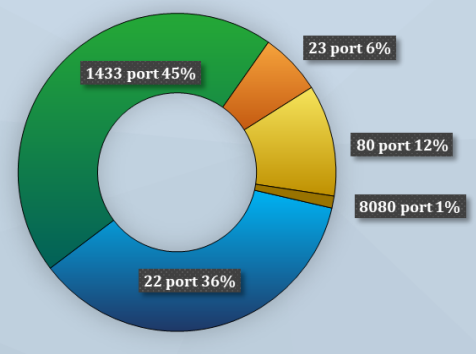
Fenyegetettségi szint: alacsony



Incidensek eloszlása típus és kockázati besorolás szerint

Az elosztott kormányzati IT-biztonsági csapdarendszerből (Gov1probe) származó adatok:





További információkért, látogasson el **weboldalunkra**!