NEMZETI KIBERBIZTONSÁGI INTÉZET

HÍRLEVÉL

Nemzetközi
IT biztonsági sajtószemle
2026. 30. hét

KONTAKT

edt@nki.gov.hu

FBC3 88A2 BF51 AD58
A2D0 E9DD E078 ABD3
E75D

nki.gov.hu

AKTUÁLIS TARTALMAK

- HÍREK
- STATISZTIKAI ADATOK
- RIASZTÁS

További érdekességekért és IT biztonsággal kapcsolatos tartalmakért látogasson el LinkedIn oldalunkra vagy hallgassa meg podcast adásainkat!

KIBERTÁMADÁS! PODCAST

NEMZETI KIBERBIZTONSÁGI INTÉZET

HÍREK

A Fortinet sérülékenységek javítását sürgeti a CISA

(bleepingcomputer.com)

A CISA arra szólította fel a kormányzati ügynökségeket, hogy kezeljék prioritásként a Fortinet FortiSandbox fenyegetésészlelő platform két aktívan kihasznált sebezhetőségét. A szóban forgó CVE-2026-39808 és CVE-2026-25089 azonosítón nyilvántartott sebezhetőségek alacsony komplexitású parancsbefecskendezési (OS command injection) támadással jogosulatlan távoli kódfuttatást tesznek lehetővé, felhasználói beavatkozás nélkül. **Bővebben...**

Nyilvánosságra kerültek a WordPress Core „wp2shell” RCE sérülékenységeinek PoC exploitjai

(bleepingcomputer.com)

Nyilvánosságra kerültek a kritikus súlyosságú „wp2shell” néven ismert, távoli kódfuttatást (Remote Code Execution, RCE) lehetővé tevő WordPress Core sérülékenységekhez készült proof-of-concept (PoC) exploitok, ezért a rendszergazdáknak javasolt haladéktalanul frissíteniük az érintett rendszereket. **Bővebben...**

Több sérülékenység javítását tartalmazó frissítést adott ki a Zimbra

(thehackernews.com)

A Zimbra kiadta a 10.1.20-as verziót, amely több sérülékenység javítását tartalmazza. A frissítés egyik legfontosabb eleme a Simple Network Management Protocol (SNMP) komponenst érintő, command injection sérülékenység javítása. A hiba az SNMP felügyeleti modulban található, és akkor használható ki, ha az SNMP-értesítések engedélyezve vannak. **Bővebben...**

Zsarolóvírus terjesztésére használják a GlobalProtect VPN hibát

(bleepingcomputer.com)

A Palo Alto Networks GlobalProtect VPN-jének egy kritikus, hitelesítés-megkerülő sérülékenységét a Qilin zsarolóvírus csoport vállalati hálózatok feltörésére használja fel.
Bővebben...

Megzsarolták a Stadlert

(bleepingcomputer.com)

A svájci vasúti járműgyártó szerint az Everest ransomware-csoport 12,3 millió dollárt követelt tőlük. A támadás az egyik beszállítójával közösen használt adatcsere-platformon keresztül történt. Az esetet még az Everest csoport nem vállalta magára, de a Stadler feljelentést tett a thurgaui kantonális rendőrségen, miután kijelentette, hogy nem fog fizetni a zsarolóknak.
Bővebben...

NEMZETI KIBERBIZTONSÁGI INTÉZET

STATISZTIKAI ADATOK

2026. 07. 17. - 2026. 07. 23.

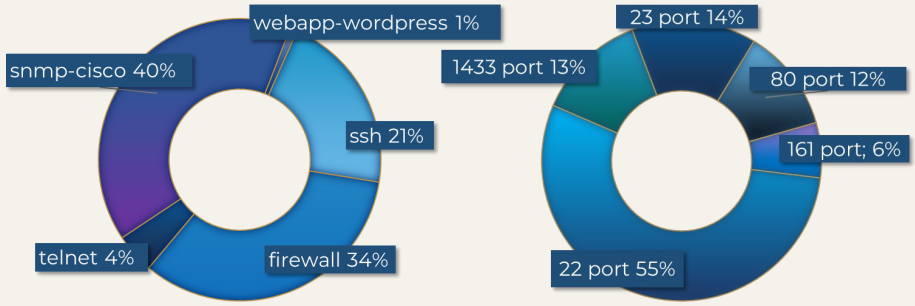
Fenyegetettségi szint:

alacsony | közepes | magas | kritikus

Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok

Az adatsorok melletti nyilak az előző héthez viszonyított változásokat mutatják.

Az elosztott kormányzati IT biztonsági csapdarendszerből (GovProbe1) származó adatok



NEMZETI KIBERBIZTONSÁGI INTÉZET

RIASZTÁS

Riasztás Oracle szoftverek júliusban javított sérülékenységeiről

A Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet riasztást ad ki, **Oracle termékeket érintő sérülékenységek kapcsán**. Az Oracle júliusi Critical Patch Update (CPU) frissítési csomagjában összesen **1449 különböző sérülékenység került javításra**.

Kritikus sebezhetőségeket azonosítottak az Oracle számos termékeiben. Az NBSZ NKI a biztonsági frissítések **haladéktalan telepítését** javasolja.

Elolvasom

Sérülékenységek listája

Kövesse folyamatosan frissülő sérülékenység listánkat, hogy naprakész maradhasson a legújabb, és legaktuálisabb fenyegetésekkel kapcsolatban!