NEMZETI KIBERVÉDELMI INTÉZET

HÍRLEVÉL

Nemzetközi
IT-biztonsági sajtószemle
2024. 12. hét

HÍREK

- Ismeretlenek feltörték az IMF 11 e-mail fiókját
- 100 millió e-mail és Instagram fiókot törtek fel a hackerek
- Kritikus sebezhetőséget javított a Fortra
- Két sérülékenységet javított az Ivanti
- A Fortinet kritikus RCE hibára figyelmeztet

SÉRÜLÉKENYSÉGEK

- Riasztás Microsoft termékeket érintő sérülékenységekről
- Riasztás Adobe szoftverek sérülékenységeiről

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

További érdekességekért, látogasson el **weboldalunkra**!

IT biztonsági HÍREK

Ismeretlenek feltörték az IMF 11 e-mail fiókját

(bleepingcomputer.com)

A Nemzetközi Valutaalap (IMF) nyilvánosságra hozta, hogy ismeretlen támadók az év elején feltörtek 11 IMF e-mail fiókot. Ez a 190 tagország által finanszírozott nemzetközi pénzügyi intézmény egyben az ENSZ egyik legfontosabb pénzügyi szerve is, amelynek székhelye Washingtonban található. **Bővebben...**

100 millió e-mail és Instagram fiókot törtek fel a hackerek

(thehackernews.com)

Az ukrán kiberrendőrség letartóztatott három személyt, akik több mint 100 millió e-mail és Instagram fiókot törtek fel. A 20 és 40 év közötti gyanúsítottak állítólag egy szervezett bűnözői csoport tagjai, akik az ország különböző részein élnek. Ha elítélik őket, akár 15 év börtönbüntetésre is számíthatnak. **Bővebben...**

Két sérülékenységet javított az Ivanti

(bleepingcomputer.com)

Az Ivanti figyelmeztette ügyfeleit, hogy haladéktalanul javítsák ki a kritikus súlyosságú Standalone Sentry sebezhetőséget. A hibát a NATO Kiberbiztonsági Központ kutatói jelentették. **Bővebben...**

A Fortinet kritikus RCE hibára figyelmeztet

(bleepingcomputer.com)

A Fortinet befoltozta a FortiClient EMS kritikus sebezhetőségét, amely lehetővé teszi a távoli kódfuttatást (RCE) a sebezhető szervereken. **Bővebben...**

FORTRA™

Kritikus sebezhetőséget javított a Fortra

(securityaffairs.com)

A Fortra javított egy kritikus távoli kódfuttatási sebezhetőséget, amely a FileCatalyst fájlátviteli termékeit érinti. A CVE-2024-25153 (CVSS érték: 9.8) néven nyomon követett kritikus sebezhetőség kihasználásával a támadók egy távoli, tetszőleges kódot futtathatnak az érintett szervereken a hitelesítés megkerülésével.

Bővebben...

TÁJÉKOZTATÓK, SÉRÜLÉKENYSÉGEK, RIASZTÁSOK

Riasztás Microsoft termékeket érintő sérülékenységekről

A Microsoft 2024. március havi biztonsági csomagjában összesen **61** különböző **biztonsági hibát javított**, köztük **2 kritikus** kockázati besorolású sebezhetőséget, amelyek kihasználása távoli kódfuttatást, szolgáltatásmegtagadást, jogosulatlan adathozzáférést és jogosultság kiterjesztést tesz lehetővé a sérülékeny rendszeren. A javított sérülékenységek között **nulladik napi (zero-day)** sebezhetőség nem található.

Elolvasom

Tájékoztatás Adobe szoftverek sérülékenységeiről

Az NBSZ NKI **tájékoztatót** ad ki az **Adobe** szoftverfejlesztő cég **termékeit érintő sérülékenységekkel kapcsolatban**, azok súlyossága, valamint az egyes biztonsági hibákat érintő aktív kihasználások miatt.

Elolvasom

További tájékoztatókért, látogasson el **weboldalunkra**!

Aktuális tartalmak

Indul a NIS2 tájékoztató kampány [aktuális]

A NIS2-ről már eddig is sokat beszéltünk, de még mindig nem eleget! Ugyanis az óra ketyeg, a NIS2 hatálya alá eső új ágazatok szereplőinek pedig minél előbb be kell azonosítaniuk magukat érintettként.
Az SZTFH Minden Kiberül podcastjével közös adásunkban erről beszélgettünk.

Az adásban vendégeink:

Dr. Bencsik Balázs
az SZTFH kiberbiztonsági igazgatója

Bor Olivér
az SZTFH kiberbiztonsági szakértője

Orosházi Dávid
az NBSZ NKI Hatóságának főosztályvezetője

1. rész **2. rész**

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

LinkedIn

Instagram

Facebook

Statisztikai Adatok

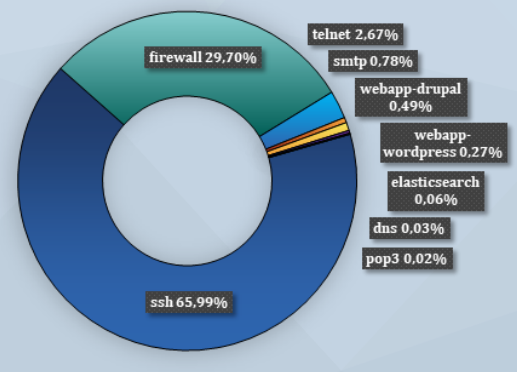
2024.03.14.-2024.03.21.

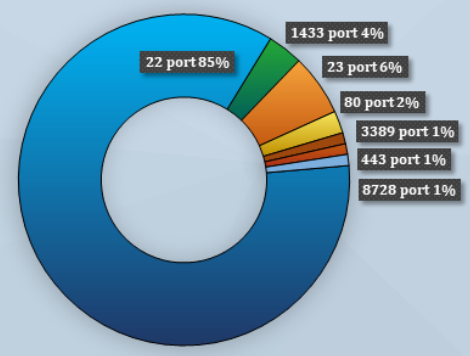
Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok:

Fenyegetettségi szint: alacsony

Incidensek eloszlása típus és kockázati besorolás szerint

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





További érdekességekért, látogasson el **weboldalunkra**!