2019

NT KONFERENCA

21. - 23. MAJ 2019

#ntk19

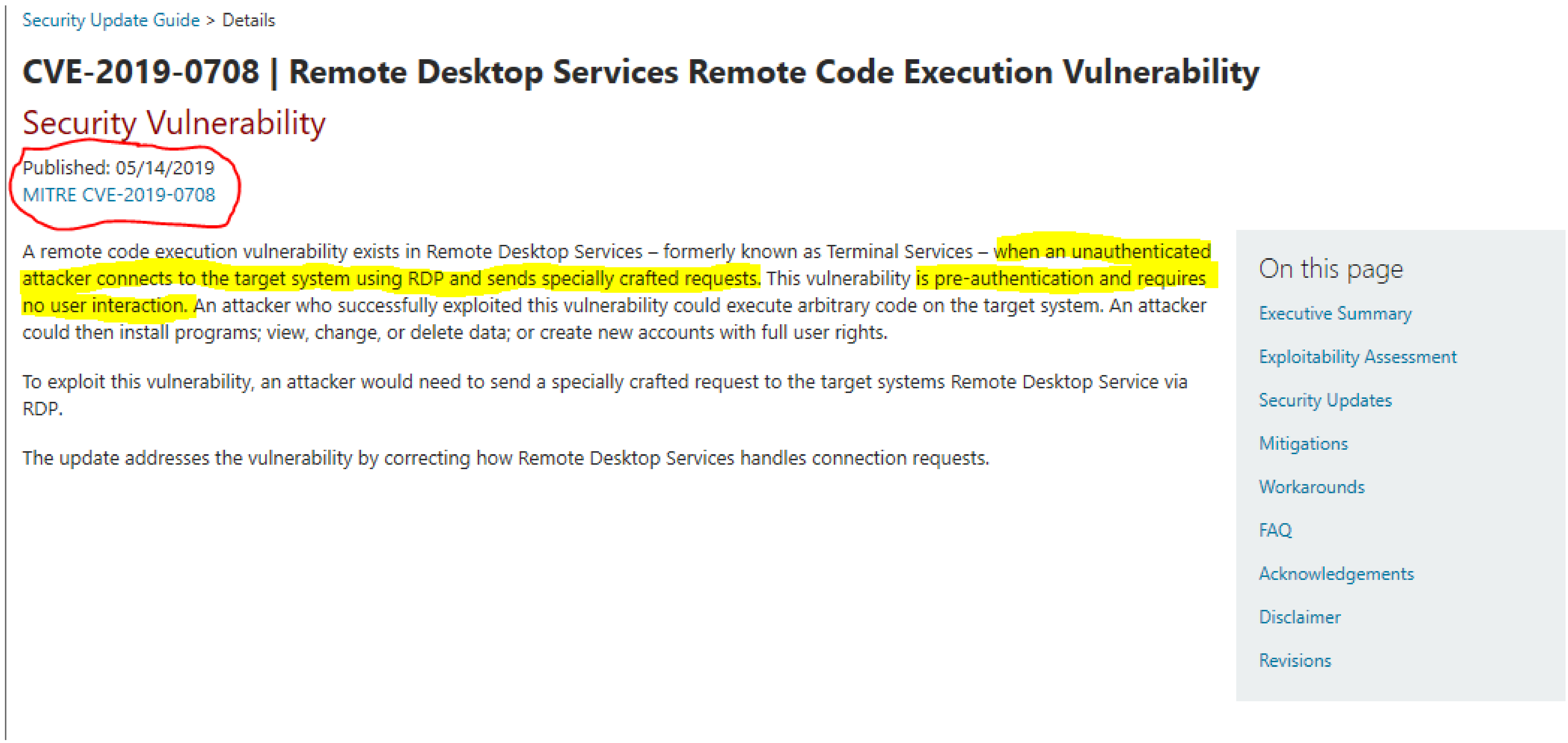
RDS Prihodnost:

Server2019, RDmi in HTML5

Elvis Guštin
EM-Soft sistemi d.o.o.

elvis@em-soft.si

Lahko takoj začnemo z novostmi:



Security Update Guide > Details

CVE-2019-0708 | Remote Desktop Services Remote Code Execution Vulnerability

Security Vulnerability

Published: 05/14/2019
MITRE CVE-2019-0708

A remote code execution vulnerability exists in Remote Desktop Services – formerly known as Terminal Services – when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests. This vulnerability is pre-authentication and requires no user interaction. An attacker who successfully exploited this vulnerability could execute arbitrary code on the target system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

To exploit this vulnerability, an attacker would need to send a specially crafted request to the target systems Remote Desktop Service via RDP.

The update addresses the vulnerability by correcting how Remote Desktop Services handles connection requests.

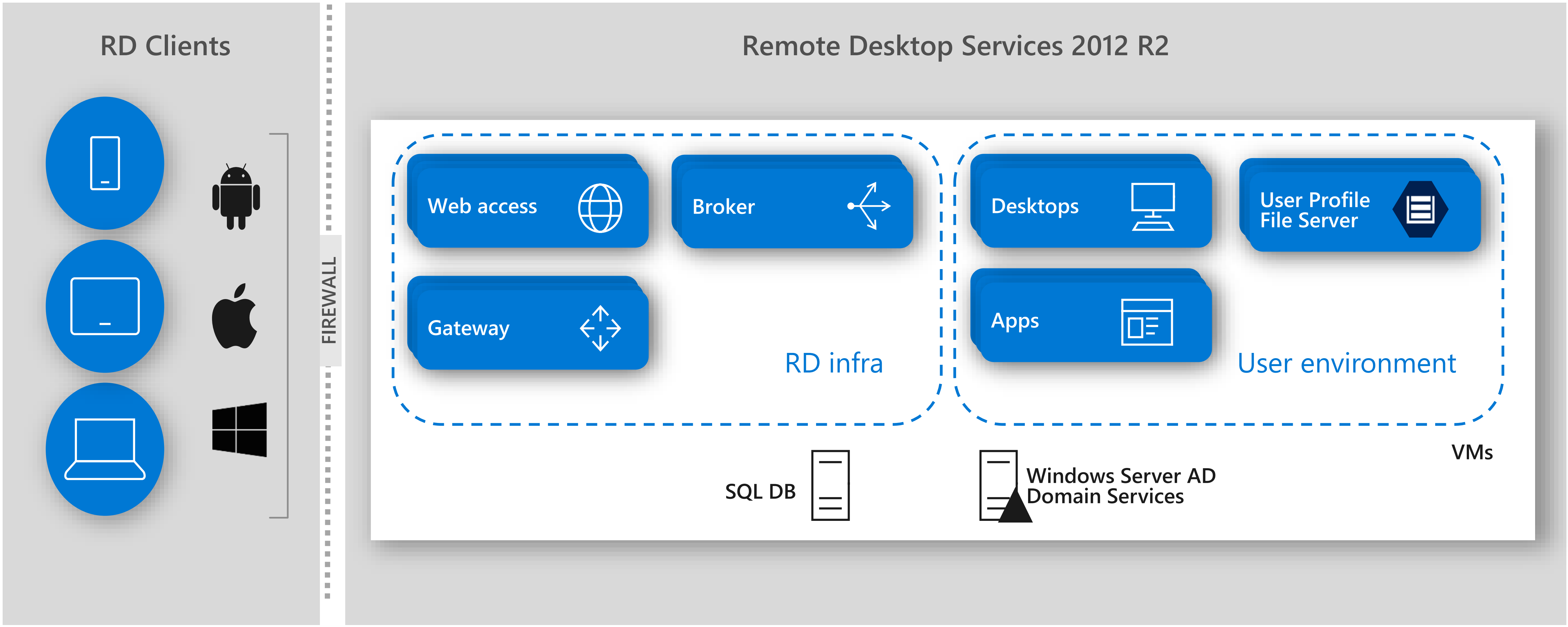
On this page

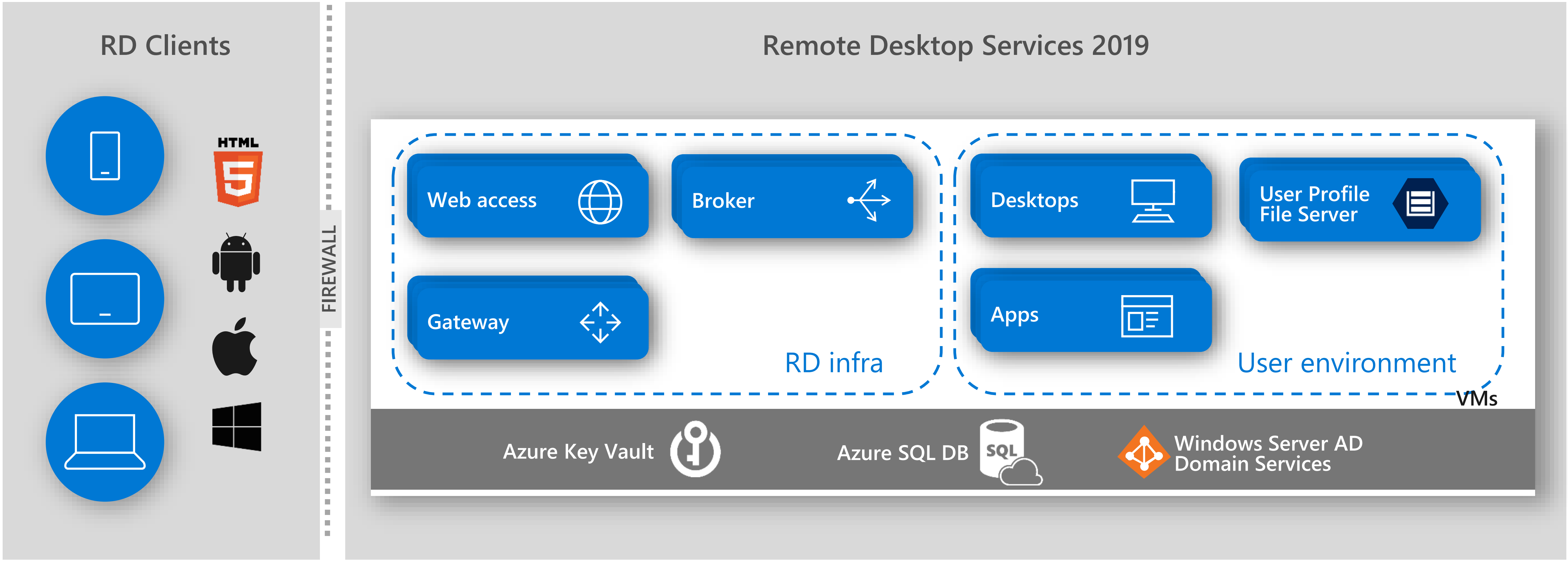
- Executive Summary
- Exploitability Assessment
- Security Updates
- Mitigations
- Workarounds
- FAQ
- Acknowledgements
- Disclaimer
- Revisions

Minuta zgodovine

- Do Serverja 2003 je bila RDS ena vloga
  - Problemi s farmami
  - Problemi s tiskalniki
  - V glavnem uporabljena v kombinacijami z drugimi produkti (Citrix)
- Server 2008 krepko spremeni strategijo
  - Prihaja 5 vlog
  - Easyprint funkcionalnost
  - Remote App tehnologija
  - Profile diski
  - Kasneje še podpora strojni opremi in nove funkcije (Grafične kartice,…)
- Do verzije Server 2019 so samo manjši koraki naprej – a ne nepomembni

Od 2012R2 do 2019





Zakaj toliko poudarka na Azure?

- Microsoft stavi veliko na Azure
- RDS pomeni delo od kjerkoli, torej je Cloud prava izbira
- Zabeležena rast YoY je več kot 230% in stalno raste
- RDS tehnologija trenutno rabi približno 10% compute moči v Azure-u
- Hitro podajanje novih funkcij in prilagajanje uporabniku

Novosti v verziji 2019

- Html5 vmesnik (možen že na verziji 2016!)
  - Vedno več servisov bo prestavljenih na web – tudi zaradi Cloud-a
  - Lepše delovanje Remote App-ov
  - Enostavna instalacija in ne omejuje drugih načinov delovanja

    https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/clients/remote-desktop-web-client-admin
  - Zahteve niso hude
    - Javni certifikat
    - Windows 10 ali Server 2008R2 klienti
    - Per User licenčni model (Per device bo porabil vse licence!)
  - Dostop na https://vstopnatocka/rdweb/webclient/index.html (boste uredili redirect?)

Graphics virtualization technology

Windows Server 2012 R2

RemoteFX vGPU

- DX 11.1 support
- Higher video memory
- Up to 2560 × 1600 resolution
- Scale improvements

Windows Server 2016

RemoteFX vGPU

- OpenGL 4.4/OpenCL 1.1
- 1 GB dedicated VRAM
- Up to 4K resolution
- Server VM support

Discrete Device Assignment (DDA)

- Native GPU driver support
- Full API support

Windows Server 2019

DDA

- Improved RDSH scalability with GFX HW acceleration
- Use all available GPUs
- Improvements on video detection and handling
- Region classification improvements
- High DPI downsampling

DDA and RemoteFX vGPU in WS2019

DDA

- Primary story for GPU acceleration in WS2019
- Enhanced security and isolation
- Guaranteed GPU performance
- API compatibility (DirectX 12, OpenGL)
- We are continuing to evaluate GPU-P drivers for VDI and RDSH

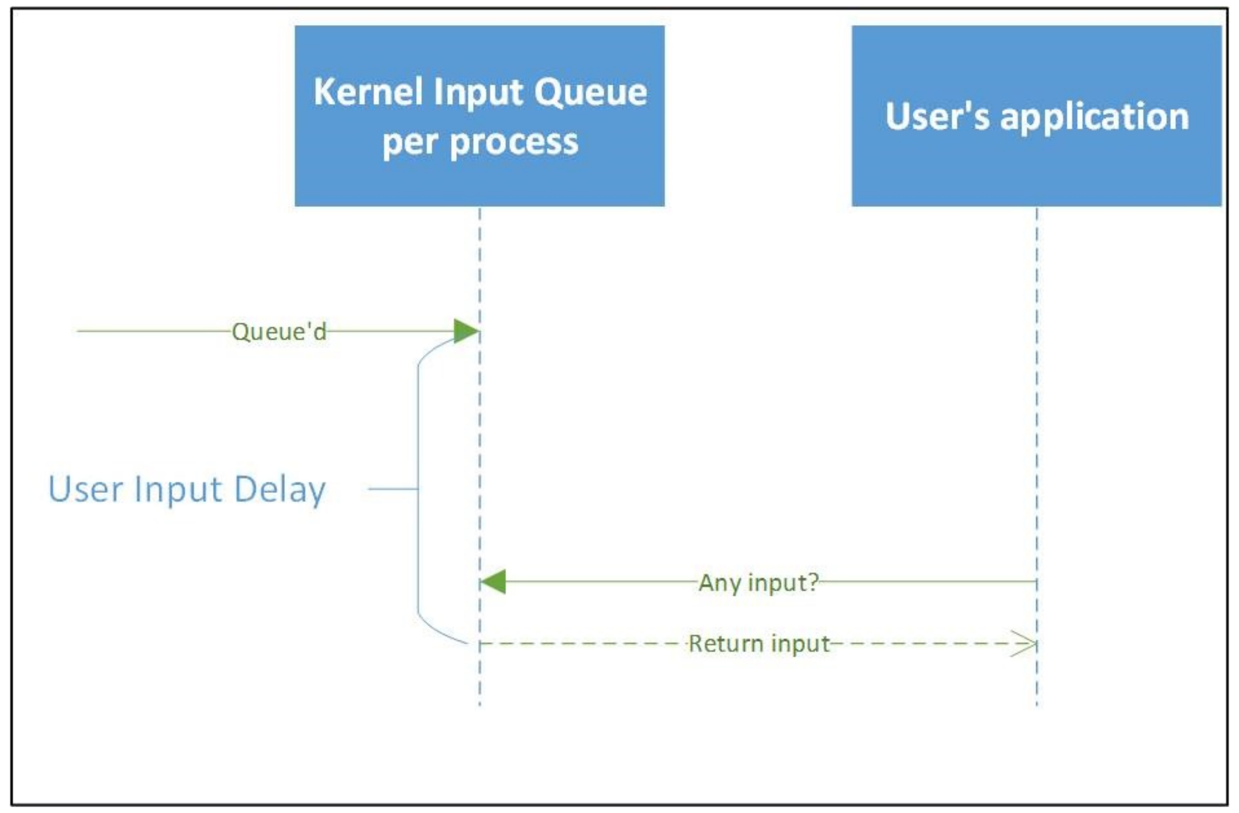
RemoteFX vGPU

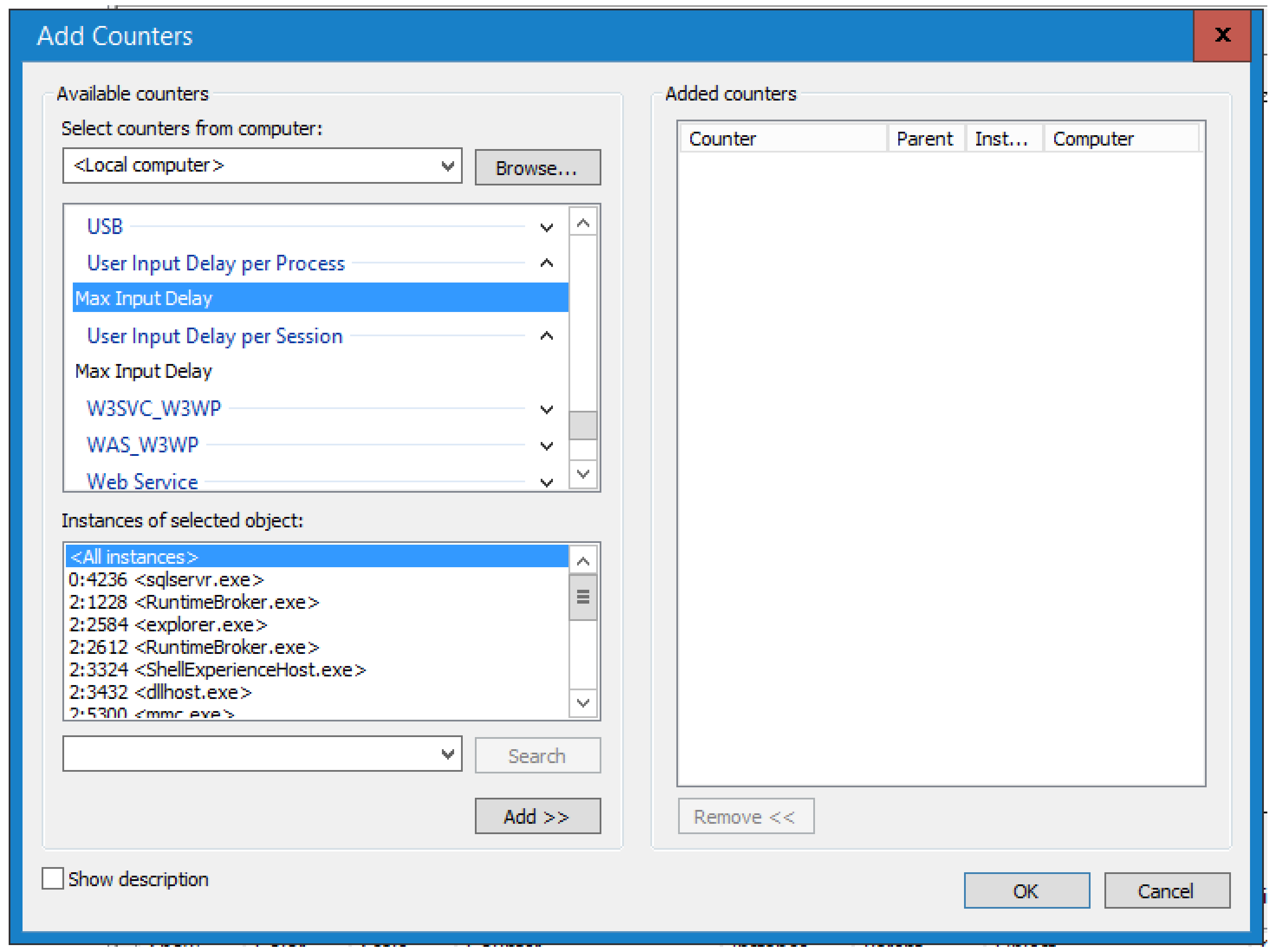
- Deprecated in WS2019
- Clean OS installation cannot share RemoteFX vGPUs with new Hyper-V VMs
- Upgrade warning if RemoteFX vGPU is enabled in the upgraded OS
- If you had a RemoteFX vGPU-enabled VM it will continue to work after upgrade
- Admins can remove RemoteFX vGPU after upgrade to WS2019

User Input Delay performance counters

- Način merjenja in odkrivanja vzrokov slabe odzivnosti
- Delujejo skupaj z drugimi counterji (Active Sessions, CPU, …)
- So že vgrajeni v Windows 10 1809, Server 2019,…

  https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/rds-rdsh-performance-counters
- Uporabni pri iskanju problemov odzivnosti




Add Counters

Available counters

Select counters from computer:

<Local computer>

Browse...

USB
User Input Delay per Process
Max Input Delay
User Input Delay per Session
Max Input Delay
W3SVC_W3WP
WAS_W3WP
Web Service

Instances of selected object:

<All instances>
0:4236 <sqlservr.exe>
2:1228 <RuntimeBroker.exe>
2:2584 <explorer.exe>
2:2612 <RuntimeBroker.exe>
2:3324 <ShellExperienceHost.exe>
2:3432 <dllhost.exe>
2:5300 <mmc.exe>

Search

Add >>

Added counters

Counter	Parent	Inst...	Computer

Remove <<

☐ Show description

OK

Cancel

Migracija iz verzije 2008+

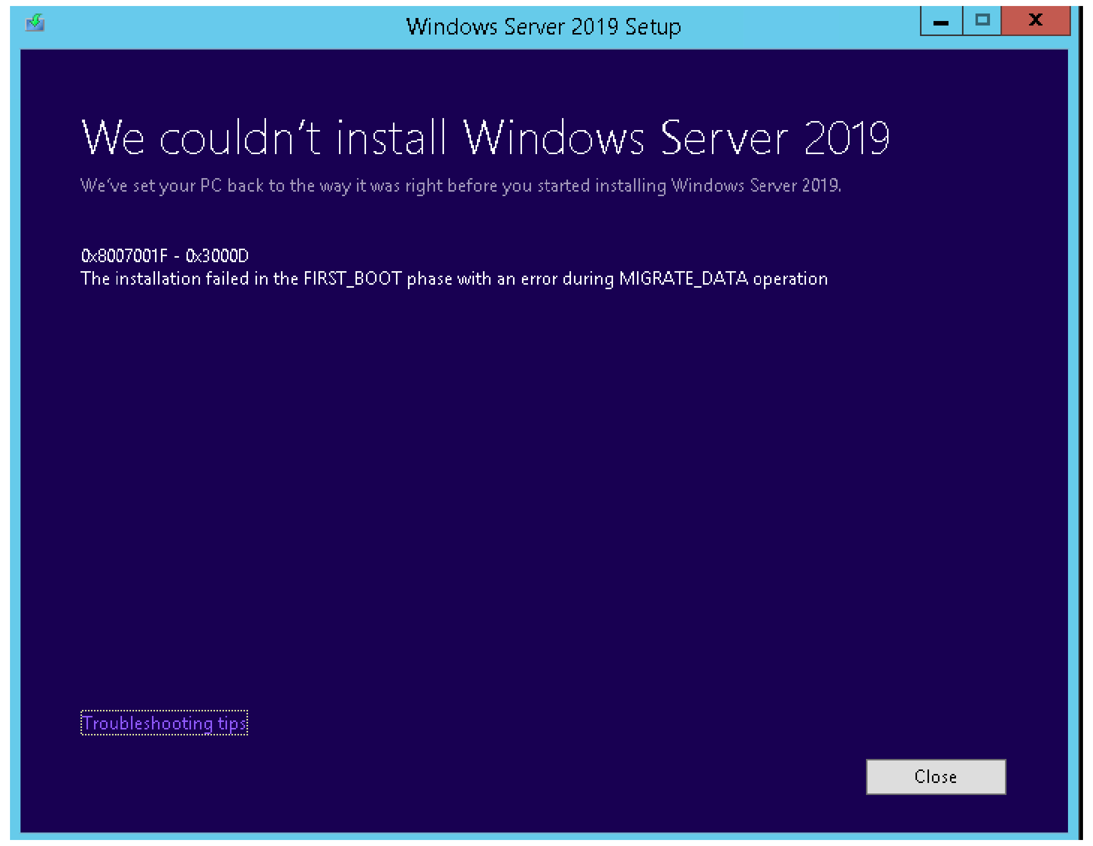
- Uporabljajte glavo in precej razmislite kako boste postopali
- Aplikacije, ki jih uporabljate ni nujno da delujejo

  (ja, imel sem že 16 bitne DOS aplikacije, ki so delovale na 32 bitni OS platformi)
- Če je farma majhna, se splača delati migracijo?
  - Inplace upgrade ni nujno da je vedno uspešen
    - Aplikacije ostanejo instalirane
    - User profiles so še vedno tam
    - Življenje sistema ostane – kaj že ste delali po registrih, file-ih,…
    - Nujno testno okolje!
  - Side-by-side migracija je precej lažja, vendar skriva pasti
    - Connection broker, prilagoditve WEB vmesnika, profile diski,…
    - Namestitve aplikacij

Problemi in-place migracije

Temp profili na strežniku

- Preverite pred migracijo in jih brišite (če obstajajo)
- Problemi v primeru prehoda na Profile Diske



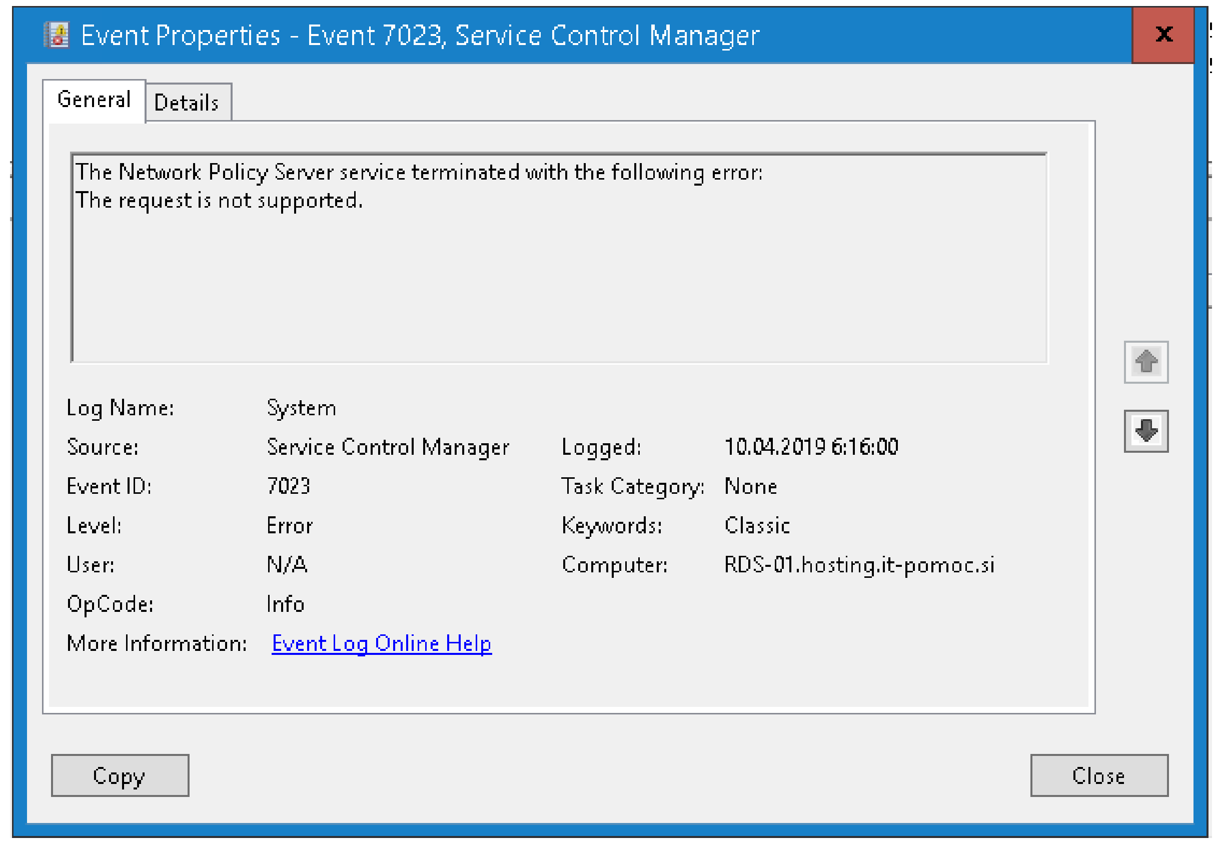
We couldn't install Windows Server 2019

We've set your PC back to the way it was right before you started installing Windows Server 2019.

```
0x8007001F - 0x3000D
The installation failed in the FIRST_BOOT phase with an error during MIGRATE_DATA operation
```

RD Gateway

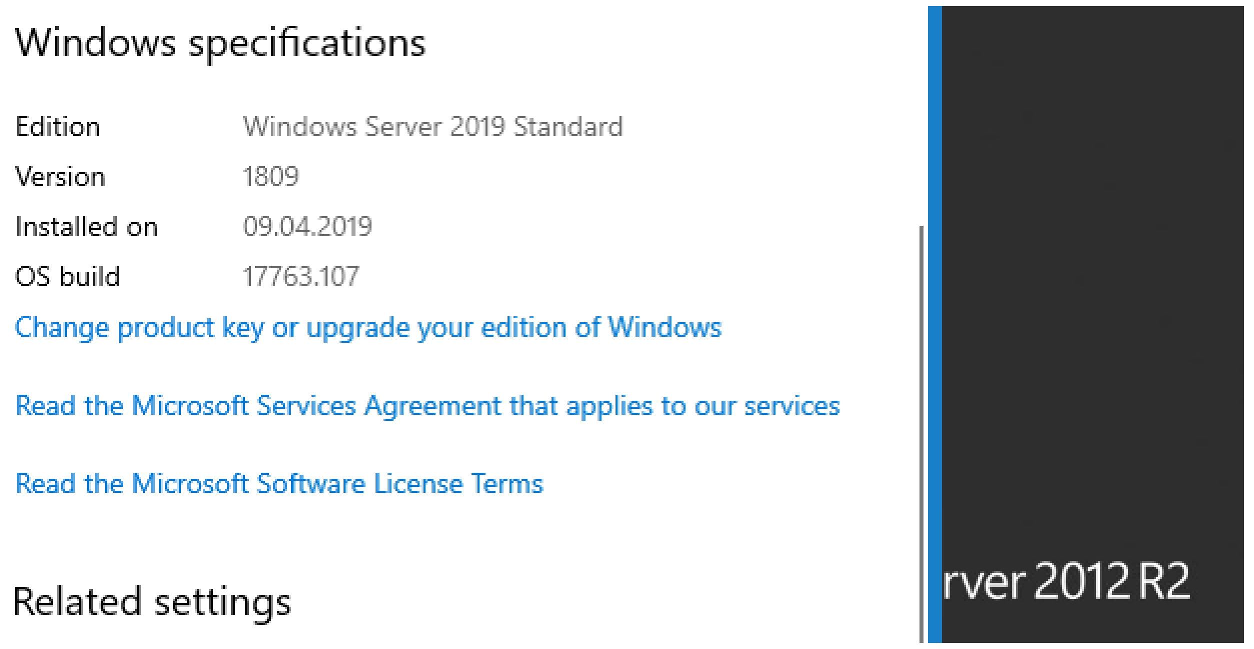
- Včasih pride do problemov z Network Policy servisom



```
The Network Policy Server service terminated with the following error:
The request is not supported.

Log Name:          System
Source:            Service Control Manager     Logged:          10.04.2019 6:16:00
Event ID:          7023                        Task Category:   None
Level:             Error                       Keywords:        Classic
User:              N/A                         Computer:        RDS-01.hosting.it-pomoc.si
OpCode:            Info
More Information:  Event Log Online Help
```

Kozmetični problemi



Windows specifications

Edition	Windows Server 2019 Standard
Version	1809
Installed on	09.04.2019
OS build	17763.107

Change product key or upgrade your edition of Windows
Read the Microsoft Services Agreement that applies to our services
Read the Microsoft Software License Terms
Related settings
rver 2012 R2

Side –by –side migracija

- Connection broker
  - Farma ima lahko NATANČNO en Connection broker
  - Ne morete ga dodati, ne morete ga odstraniti. (ročno preko rules ne deluje!)
  - MS priporoča HA implementacijo
  - Powershell skripta na https://www.cloud-architect.be/2018/07/25/migrate-your-rds-deployment-to-a-new-connection-broker-even-on-azure/
- Prilagoditve web vmesnika
  - Večina prilagoditev se dela ročno v datotekah

    login.aspx, password.aspx

    webscrips-domain.js, renderscripsts.js
  - Login.aspx je precej spremenjena – ne gre copy / paste
  - Logotipi in grafično oblikovanje ni problem
- Kolekcije in dostopi ne delajo problemov (pazite na način instalacije)

DEMO

končno

elvis@em-soft.si

Vprašanja

Elvis Guštin
EM-Soft sistemi d.o.o.

elvis@em-soft.si