

Workplace Ninja User Group Finland

31.8.2024



Workplace Ninja
User Group Finland

Kesän ajankohtaisia asioita

Petri Paavola/Panu Saukko





Ohjelma

- **Intune Device Preparation**
- **Intunen uudet ja tulevat ominaisuudet**
- **BlackLotus UEFI:n korjaukset**
- **CrowdStrike BSOD case**
- **Windows ja ARM**



Intune Device Preparation

- Uusi UI
- Hyvää:
 - Nopea
 - Mukava käyttöliittymä
 - Koneen tenant rekisteröinti kirjautumisen jälkeen
 - Koneiden rekisteröinti helpompaa (sarjanumero, IT voi tehdä itse)
 - Nopea raportointi
- Puutteita:
 - Vain käyttäjäkohdennus: uhka vai mahdollisuus?
 - Samalla käyttäjällä useita erityyppisiä koneita?
 - Ei koneiden nimeämistä
 - Pitää klikkailla tyhmät OOBEn ilmoitukset
- [Autopilot vs Device Preparation](#)
- [Keskustelu](#) Device preparationista



Peten nopea demo

www.wpninjas.fi

Muutama kuva uudesta
asennusprosessista ja profiilista





Intunen uudet ominaisuudet

- Muutamia nostoja kesän Intune-uudistuksissa
- Portaalin käyttöliittymä By platform
- Filter operatingSystemVersion ja vertailut
 - Käyttisversiossa mahdollista -gt/-ge/-lt/-le
 - Helpompi tehdä filter Windows 11 21H2 ja uudempi
 - Ei tue Preview:ta 😞
- Filter: cpuArchitecture
- Hienojakoisempia tietoturvan käyttöoikeuksia
 - App Control for Business
 - Attach surface reduction
 - Endpoint detection and response
- Discovered apps näyttää sovelluksen julkaisijan
- Uusi IME AppWorkload.log tiedosto
- Account protection profile
 - Device Guard ja WHfB asetukset samassa profiilissa

Create a filter rule based on the Intune device Operating System version. Specify a version value for the Operating System version (using -eq, -ne, -gt, -ge, -lt and -le operators) Example 1:(device.operatingSystemVersion -eq 15.7.1), Example 2: (device.operatingSystemVersion -gt 10.0.22000.1000) Example 3: (device.operatingSystemVersion -le 10.0.22631.3235).

it creating filters ↗

operatingSyste... GreaterThan 10.0.22621 ✓

Monitor | Discovered apps ...

Search × << Refresh ↓ Export Columns ▾ 9 items

App licenses

Discovered apps adobe ⓘ

App install status

App Protection status

App Configuration Status

Application name ↑	Platform	Application version	Device count	Application publisher
Adobe Acrobat (64-bit)	windows	24.003.20054	1	Adobe
Adobe Acrobat (64-bit)	windows	24.003.20054	1	Adobe
Adobe Acrobat (64-bit)	windows	24.002.20991	1	Adobe
Adobe Acrobat (64-bit)	windows	23.008.20533	1	
Adobe Acrobat Reader	windows	23.006.20320	1	Adobe Systems Incorporated
Adobe Acrobat Reader	windows	24.002.20991	1	Adobe Systems Incorporated



Intunen Suiten uudet ominaisuudet

www.wpninjas.fi

- **Enterprise Privilege Management (EPM)**
 - MSI/.ps1 tuki
 - Support Approval
 - EPM sääntöjen luonti tukipyynnön/raportin perusteella
- **Advanced Analytics**
 - Resource performance
- **Cloud PKI**
 - Delete CA
 - Pause/Resume CA
 - Revoke certificate
 - BYOCA (Bring Your Own CA)



Account-driven Apple User Enrollment now generally available for iOS/iPadOS 15+

Intune now supports account-driven Apple User Enrollment, the new, and improved version of Apple User Enrollment, for devices running iOS/iPadOS 15 and later. This new enrollment method utilizes just-in-time registration, removing the Company Portal app for iOS as an enrollment requirement. Device users can initiate enrollment directly in the Settings app, resulting in a shorter and more efficient onboarding experience.

For more information, see [Set up account driven Apple User Enrollment on Microsoft Learn](#).

Apple has announced they are ending support for profile-based Apple User Enrollment. As a result, Microsoft Intune will end support for Apple User Enrollment with Company Portal shortly after the release of iOS/iPadOS 18. We recommend enrolling devices with account-driven Apple User Enrollment for similar functionality and an improved user experience.



macOS uudistuksia

- Available DMG/PKG sovellukset macOS Company Portalissa
- Platform [SSO](#) tuki
- Paljon uusia asetuksia



Lior Bela @BelaLior · 23. heinäk.



Heads up, Device Inventory for Intune (included in Intune Core/P1) is coming in only a few months! You will be able to pull device attributes which will help with device targeting. Stay tuned for the official date but in the meantime, get excited.

[#MSintune](#) [#CloudNative](#)



Workplace Ninja Event esitys

Intune Device query and Device inventory: Your ultimate troubleshooting tools

📅 Wednesday September 18, 2024 16:40 - 17:40 CEST

📍 TBA

BlackLotus UEFI-haavoittuvuus

CVE-2023-24932





- Mega [KB5025885](#)

Take Action

For this release, the following steps should be followed:

Step 1: Install the Windows security update released on or after July 9, 2024, on all supported versions.

Step 2: Evaluate the changes and how they affect your environment.

Step 3: Enforce the changes.

Bootable media

It will be important to update bootable media once the Deployment Phase begins in your environment.

Guidance for updating bootable media is coming with future updates to this article. See the next section to create a USB thumb drive for recovering a device.



- ☑ Enable TSDebugMode
- ✔ Check for at least 2024-07 CU
- ✔ OS is not Supported - Needs to be Updated
- 📁 OSSupported
 - 📁 Pre-Check
 - ✔ Confirming if DB Updated Successfully
 - ✔ Confirming if Boot Manager Updated Succ
 - ✔ Confirming if DBX file updated Successfully
 - 📁 Determine if Remediation Needed
 - ✔ Set RunRemediation Logic

- 📁 Remediation
 - ✔ Disable BitLocker 10 Reboots
 - 📁 Step 1 Install the updated certical
 - ✔ Set AvailableUpdates 0x40
 - ✔ Restart Computer 1 of 9
 - ✔ Restart Computer 2 of 9
 - ✔ Wait a Minute to ensure Change is Cor
 - ✔ Confirming if DB Updated Successfully
 - ✔ Confirmed!! DB Updated Successfully
 - ✔ Unable to Confirm if DB Updated Prop
 - 📁 Step 2 Update the Boot Manager
 - ✔ Set AvailableUpdates 0x100
 - ✔ Restart Computer 3 of 9
 - ✔ Restart Computer 4 of 9
 - ✔ Wait a Minute to ensure Change is Cor
 - ✔ Confirming if Boot Manager Updatd Su
 - ✔ Confirmed!! Boot Manager Updated S
 - ✔ Unable to Confirm if DB Updated Prop
 - 📁 Step 3 Enable the revocation of olc
 - ✔ Set AvailableUpdates 0x80
 - ✔ Restart Computer 5 of 9
 - ✔ Restart Computer 6 of 9
 - ✔ Wait a Minute to ensure Change is Cor
 - ✔ Confirming if DBX file updated Succes:
 - ✔ Confirmed!! DBX Updated Successful
 - ✔ Unable to Confirm if DBX Updated Pro
 - 📁 Step 4 Apply the SVN update to the
 - ✔ Set AvailableUpdates 0x200
 - ✔ Restart Computer 7 of 9
 - ✔ Restart Computer 8 of 9
 - 📁 CleanUp
 - ✔ Disable BitLocker 1 Reboot
 - ✔ Restart Computer 9 of 9 - LAST ONE!

- 📁 Success
 - ✔ Stamp Registry of Success
 - ✔ Write details to log
- 📁 Troubleshooting
 - ✔ Dump Variables
 - ✔ Exit with Error Code

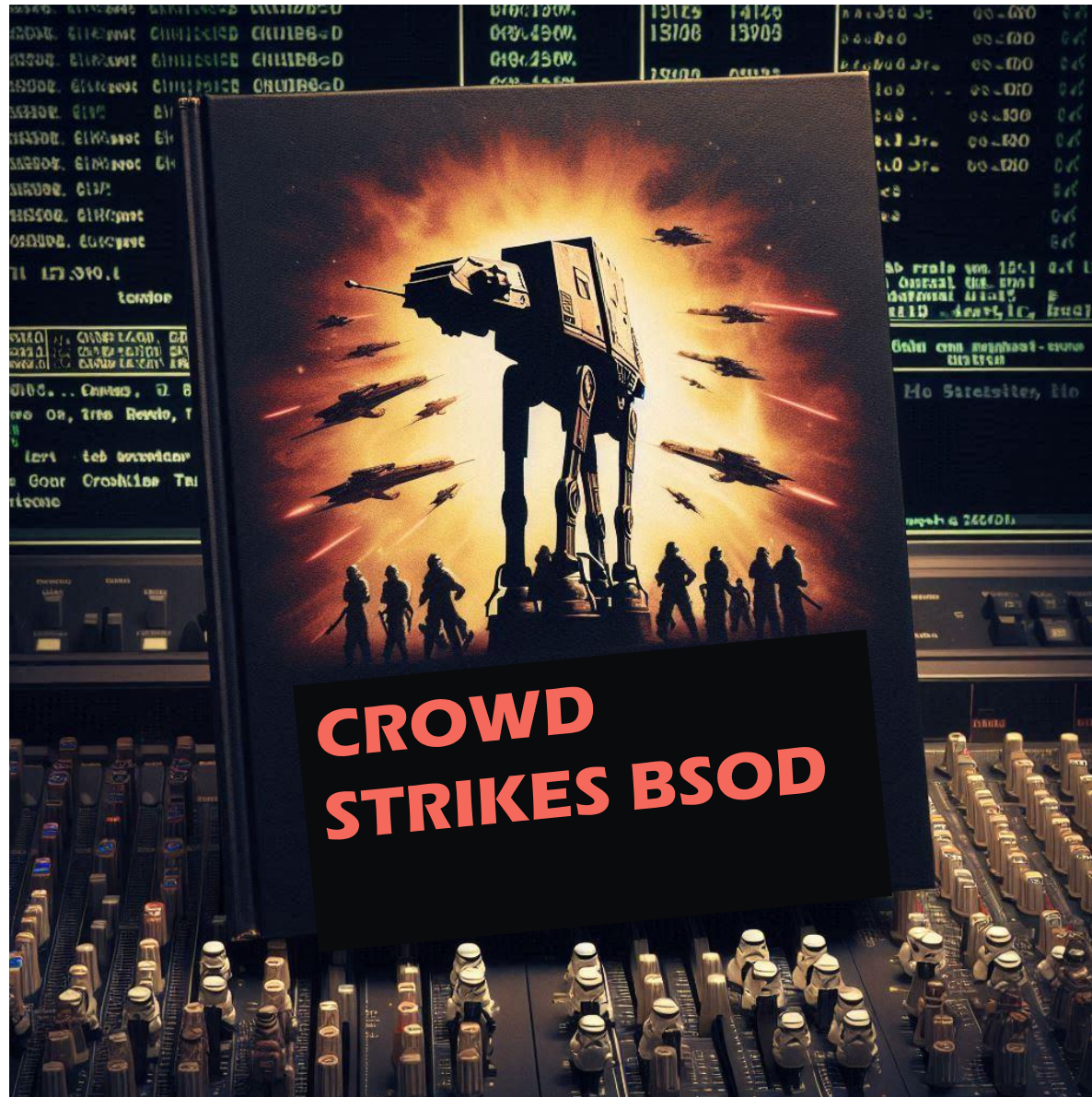
Pohjautuu Gary Blokin TS-pohjaan:

[ConfigMgr Task Sequence – KB5025885: How to manage the Windows Boot Manager revocations for Secure Boot changes associated with CVE-2023-24932 – GARYTOWN ConfigMgr Blog](#)



CrowdStrike BSOD ongelma

www.wpninjas.fi



Kosketti noin
8,5M Windows laitetta

Suomessa ei suuri
ongelma?



Ongelman syy

- CrowdStrikessa oma kernel-mode ajuri
 - Microsoftilla tiukka testausprosessi kernel-moden ajureissa → raskas prosessi
- Jotta saadaan nopeasti muutoksia haittaohjelmien tarkistukseen, ajuri hakee tekstitiedostossa konfiguraation mitä tehdä
 - Konffaustiedosto ei Microsoftin testauksen piirissä
- CrowdStrike päivitti ajuria helmikuussa havaitsemaan IPC/Named Pipe hyökkäyksiä
 - Ajurikoodi odotti 21 parametria, joista viimeinen optionaalinen
 - Konffitiedostossa vain 20 parametria
- 19.7. tuli ensimmäinen konffitiedosto, jossa viimeinen parametri ei ollut optionaalinen
 - Kuitenkin konffitiedostossa oli vain 20 parametria → out-of-memory → BSOD



Vian korjaus

- Manuaalinen korjaus
 - Fyysinen pääsy laitteelle tai iLO yms yhteys
- Koneen buuttaus Safe modeen
 - Poistetaan tiedosto `c:\windows\system32\drivers\CrowdStrike` –hakemistosta
 - Safe mode toimii vaikka Bitlocker jos buutataan levyllä
- Jos buutataan ulkoiselta medialta, silloin tarvitaan Bitlocker recovery key
- Miten löydät nopeasti Bitlocker recovery keyn?
 - Laite AD:ssä/Entra ID:ssä?
 - DC:t alhaalla?



**Koodibugeja tapahtuu:
testaus/levitysprosessin pitäisi löytää ne**



Hämmästyttävän löperö testausprosessi

“Mitä paha pelkän konffitiedoston siirrossa voi olla?”

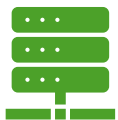
Uuden konffitiedoston globaalilevitys kaikille asiakkaille samaan aikaan

Asiakkailla ei ollut mahdollista kontrolloida Rapid Response Content-päivitysten levitystä

CrowdStriken oma testaus puutteellinen



Mitä opimme?



**Mahdollisesti meni
samaan aikaan
kaikki palvelimet
alas**

DC:t
Virtuaali-isännät
Muut palvelimet
Backup-palvelimet



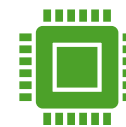
**Mistä löytyy
Bitlocker avaimet
helposti?**

Paperille? Ulkoinen levy?
Minne säilytetään?



**Paikallinen
loggautuminen
palvelimelle?**

LAPS-avaimet



Testi:

Kaikki palvelimet alhaalla
samaan aikaan → miten
ympäristö pystyyn



**Koneiden
päivitysringit**

Eri tyyppisille päivityksille

Windows ARM





Uudet Surface ARM -laitteet julkaistu - Copilot+ PCs - AI PC

- Microsoft julkaisi Buildin yhteydessä uudet Surface Pro ja Surface Laptop ARM -laitteet
- Huom! Nyt julkaistiin kuluttajamallit.
- Syksyllä tulee ARM-laitteiden business-mallit
- Ja toki kaikki muutkin isot laitevalmistajat ovat julkaisseet uudet ARM-laitteet
- Uusi prosessori tehokkaampi kuin Applen uusi M4-prosessori?
 - Qualcomm Snapdragon X Elite



Microsoftin tavoite on saada ARM-arkkitehtuuri nyt laajemmin käyttöön

AI PC:ssä tarjotaan uusia mielenkiintoisiakin ominaisuuksia



ARM-yhteensopivuus

- ARM-sovellusyhteensopivuuslinkit
 - <https://www.qualcomm.com/products/features/windowsapps>
 - <https://armrepo.ver.lt/>

Ask The Ninjas!

Kaikki





Kiitos

