Workplace Ninja User Group Finland

31.8.2024

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

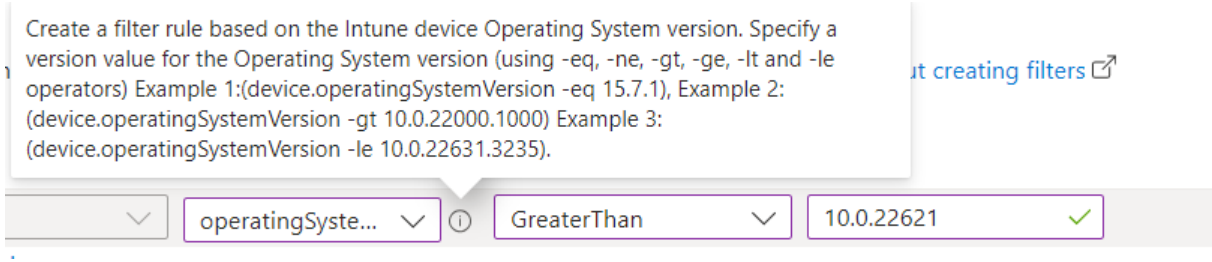
- **Uusi UI**
- **Hyvää:**
  - **Nopea**
  - **Mukava käyttöliittymä**
  - **Koneen tenant rekisteröinti kirjautumisen jälkeen**
  - **Koneiden rekisteröinti helpompaa (sarjanumero, IT voi tehdä itse)**
  - **Nopea raportointi**
- **Puutteita:**
  - **Vain käyttäjäkohdennus: uhka vai mahdollisuus?**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

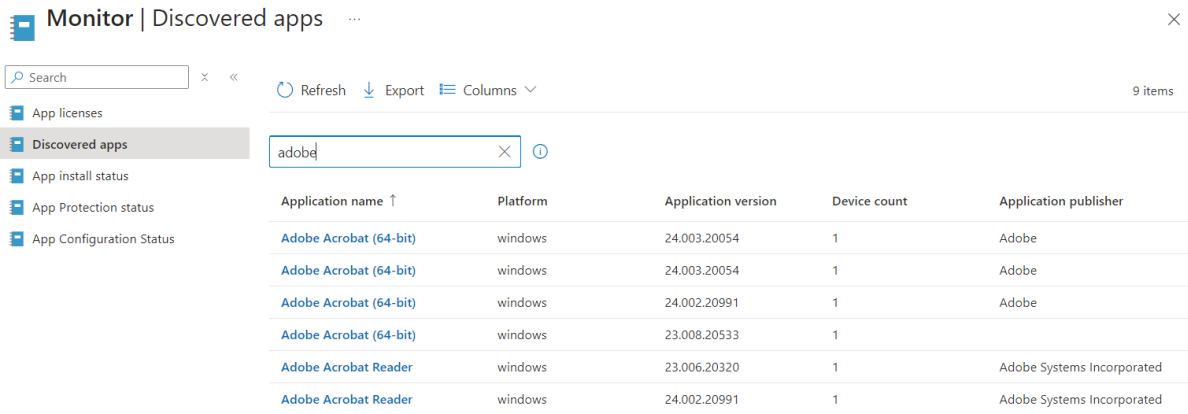
Peten nopea demo

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





Intunen Suiten uudet ominaisuudet

- 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)

iOS Enrollment uudistuksia

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.

https://learn.microsoft.com/en-us/mem/intune/enrollment/apple-account-driven-user-enrollment

macOS uudistuksia

- Available DMG/PKG sovellukset macOS Company Portalissa
- Platform SSO tuki
- Paljon uusia asetuksia

Intune huhu

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

BlackLotus UEFI korjaus

- 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.

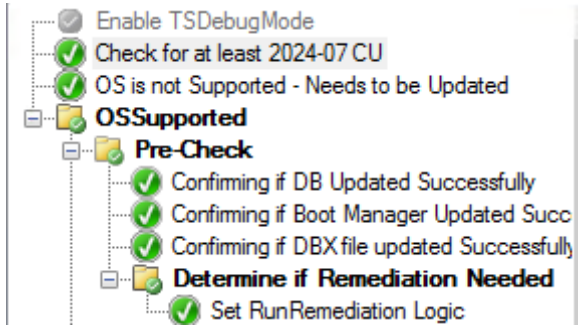
Step 3: Enforce the changes.

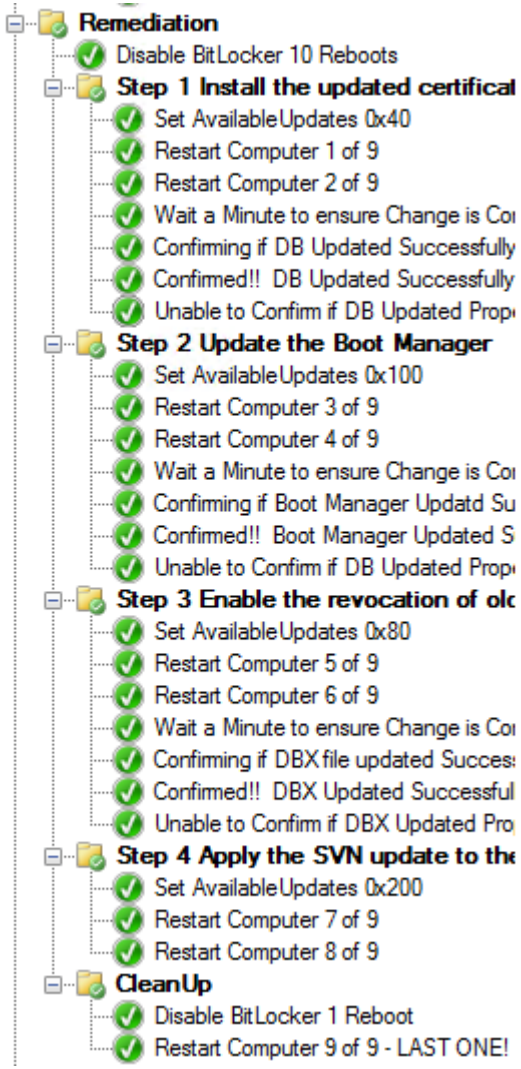
Bootable media

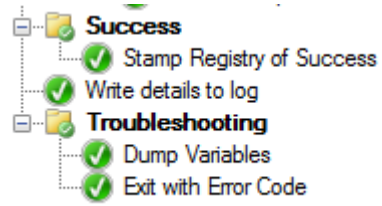
It will be important to update bootable media once the Deployment Phase begins in your environment.

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.

Korjaus



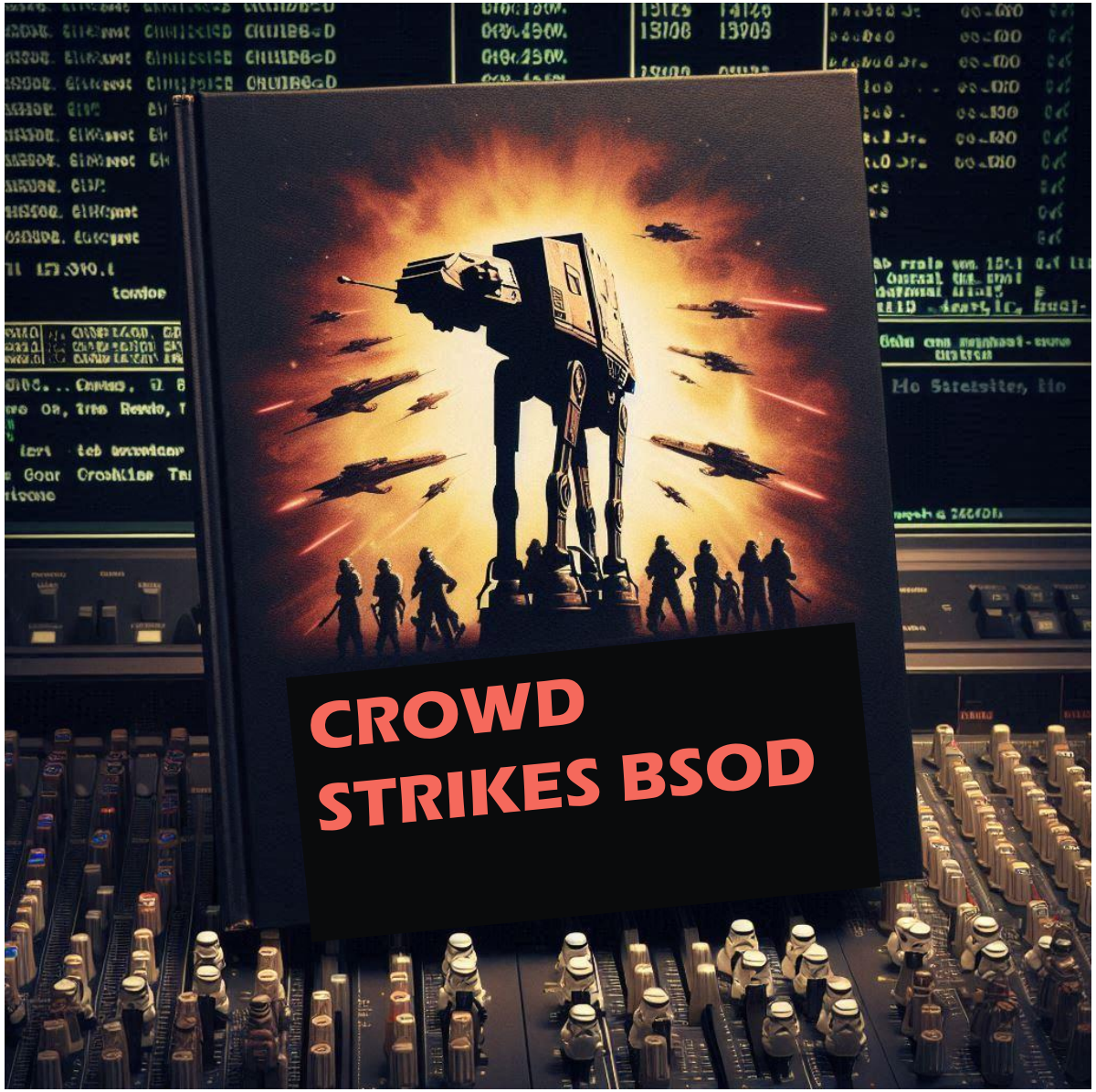




Pohjautuu Gary Blokin TS-pohjaan:

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



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?

Kysymykset

Koodibugeja tapahtuu:
testaus/levitysprosessin pitäisi löytää ne

Hämmästyttävän löperö testausprosessi

“Mitä pahaa 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

ARM-laitteet

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

Workplace Ninja
User Group Finland