# nic X edition

May 31 – June 2, Oslo Spektrum

10th anniversary

# Maintaining BIOS & Drivers updates with Intune *for real*

## Jan Ketil Skanke

Principal Cloud Architect

CloudWay

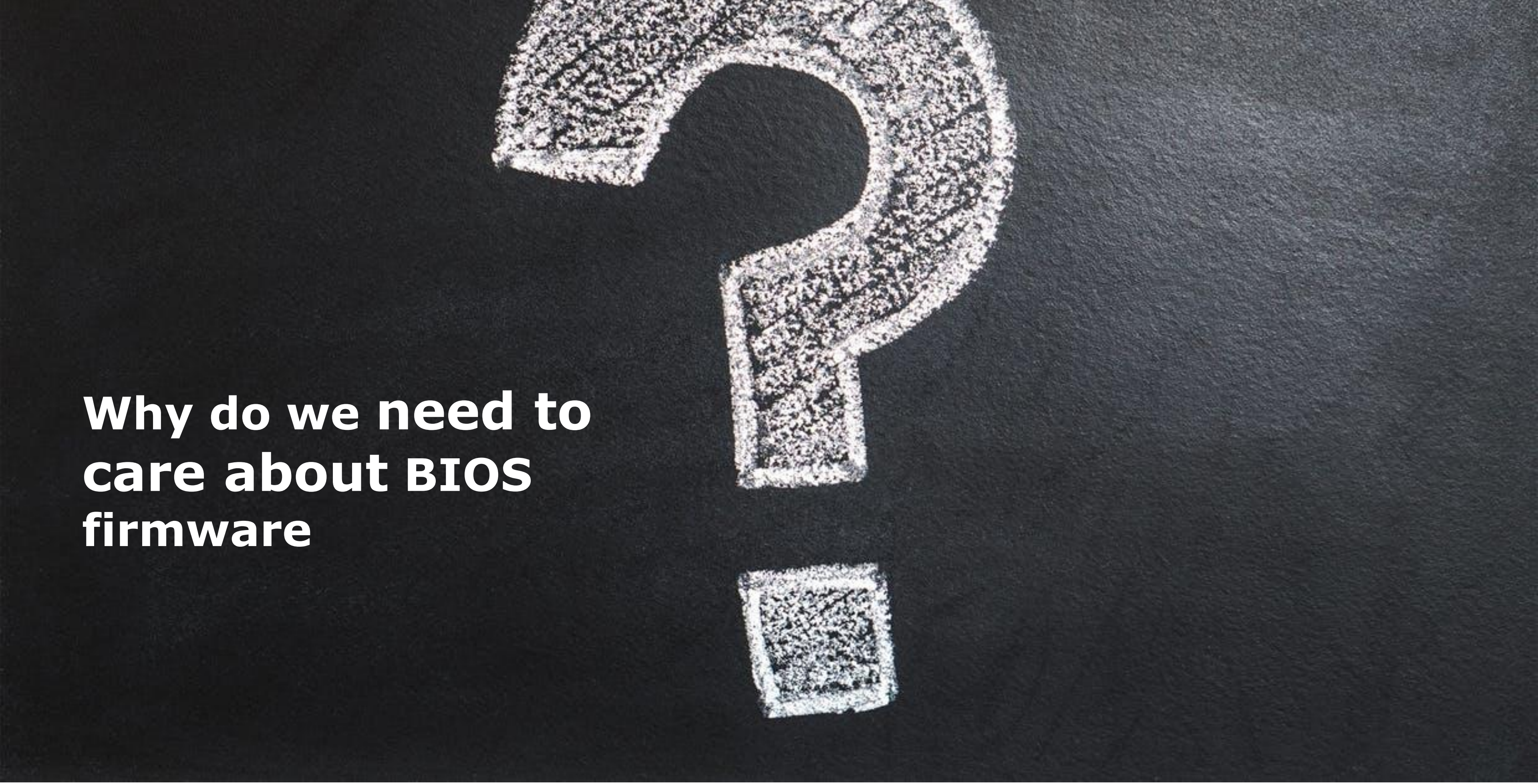
Microsoft MVP, MCT
@jankeskanke

## Maurice Daly

Principal Cloud Architect

CloudWay

Microsoft MVP, MCT
@modaly_it



# Why do we need to care about BIOS firmware

# BIOS Security Updates – Spectre / Meltdown

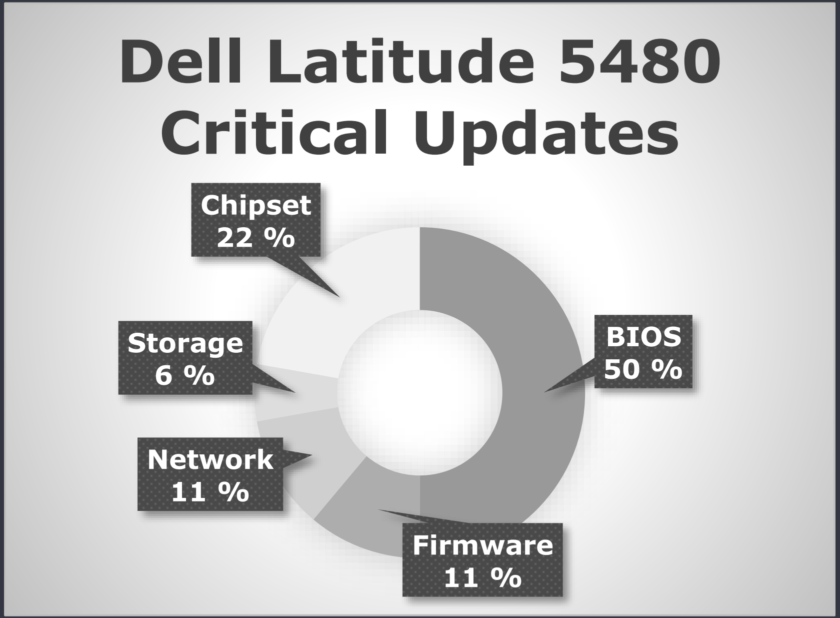
- **Traditionally** – BIOS updates were done on break/fix or re-imaging

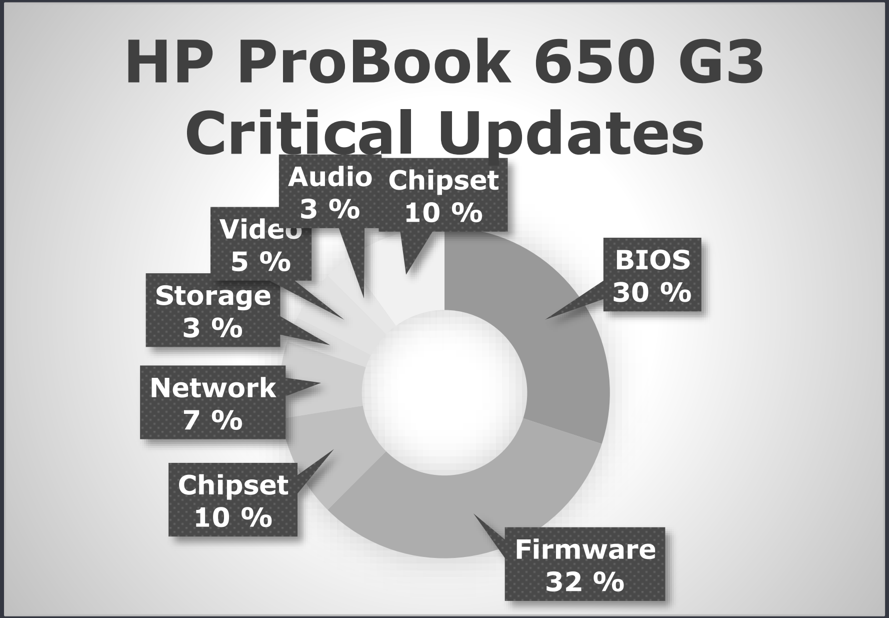
- **Then this happened..** - Spectre & Meltdown security issues announced by Intel in 2017
    - Impacting on EVERY Intel CPU since 1995, but also included AMD and ARM
    - To date this has generated 12 separate Common Vulnerabilities and Exposure notices;
      CVE-2018-3665 ; CVE-2018-3665 ; CVE-2018-3646 ; CVE-2018-3640 ; CVE-2018-3640 ; CVE-2018-3639 ; CVE-2018-3620 ; CVE-2018-3620 ; CVE-2018-3615 ; CVE-2018-1038 ; CVE-2017-5715 ; CVE-2017-5715
      https://support.microsoft.com/en-ie/help/4073757/protect-your-windows-devices-against-spectre-meltdown

- Microsoft released patches for Windows, however, this only masks the underlying issue that is within the firmware
- BIOS firmware updates released from all major vendors for supported hardware

# Updates – Drivers are my only concern..

Critical update comparison – BIOS/Drivers

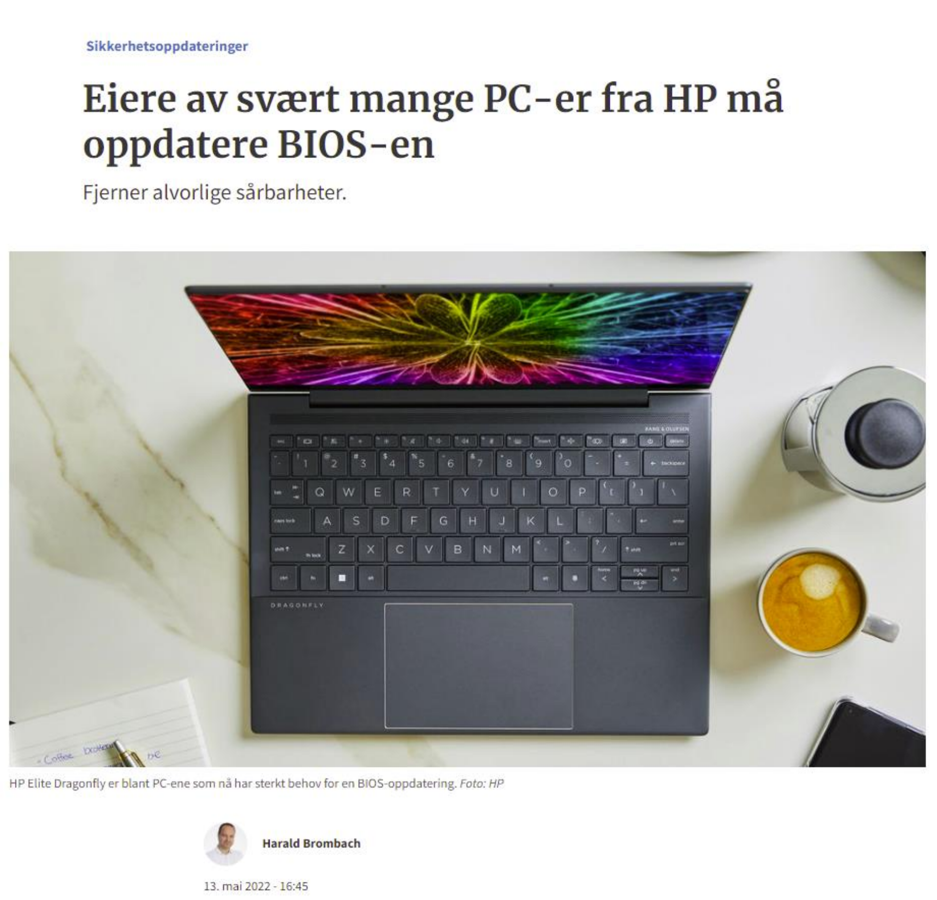




# BIOS Updates – NOT IMPORTANT??.. RIGHT??

- Manufacturers provide these updates for a reason (yes really, I'm telling the truth here)
  - Security fixes / Stability improvements
- Statistics don't lie… Lets take some popular laptop models

MPORTANT?? RIGHT??



Sikkerhetsoppdateringer

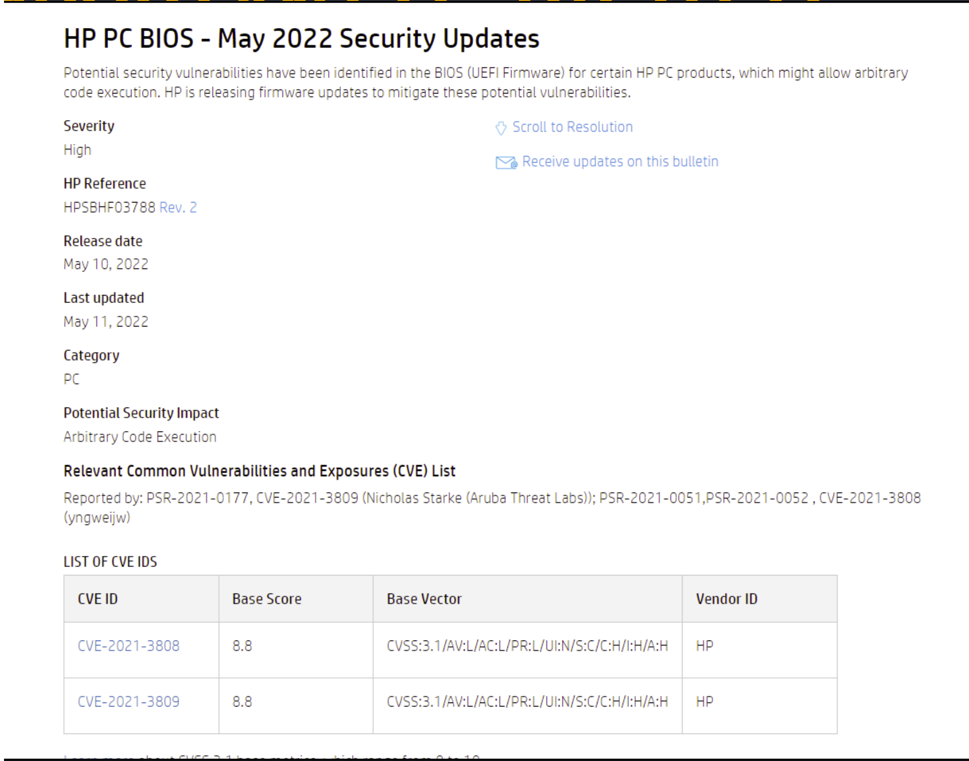
# Eiere av svært mange PC-er fra HP må oppdatere BIOS-en

Fjerner alvorlige sårbarheter.

HP Elite Dragonfly er blant PC-ene som nå har sterkt behov for en BIOS-oppdatering. *Foto: HP*

Harald Brombach

13. mai 2022 - 16:45



## HP PC BIOS - May 2022 Security Updates

Potential security vulnerabilities have been identified in the BIOS (UEFI Firmware) for certain HP PC products, which might allow arbitrary code execution. HP is releasing firmware updates to mitigate these potential vulnerabilities.

**Severity**
High

Scroll to Resolution

Receive updates on this bulletin

**HP Reference**
HPSBHF03788 Rev. 2

**Release date**
May 10, 2022

**Last updated**
May 11, 2022

**Category**
PC

**Potential Security Impact**
Arbitrary Code Execution

**Relevant Common Vulnerabilities and Exposures (CVE) List**

Reported by: PSR-2021-0177, CVE-2021-3809 (Nicholas Starke (Aruba Threat Labs)); PSR-2021-0051,PSR-2021-0052 , CVE-2021-3808 (yngweijw)

LIST OF CVE IDS

| CVE ID | Base Score | Base Vector | Vendor ID |
|---|---|---|---|
| CVE-2021-3808 | 8.8 | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H | HP |
| CVE-2021-3809 | 8.8 | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H | HP |

Learn more about CVSS 3.1 base metrics, which range from 0 to 10

# BIOS Updates – This is why YOU SHOULD CARE

**Dell XPS 15 9750**

**Version 1.24.0**

- Firmware updates to address security vulnerabilities including (Common Vulnerabilities and Exposures - CVE) such as CVE-2019-14584, CVE-2021-28210, CVE-2021-28211, CVE-2021-3712, CVE-2022-21123, CVE-2022-21125, CVE-2022-21127, CVE-2022-21166, CVE-2022-0005, CVE-2022-21151, CVE-2022-0004, CVE-2022-21181, and CVE-2021-33159.

**Version 1.22.1**

- Firmware updates to address the Intel Security Advisory INTEL-SA-00562 (CVE-2021-0157).
- Firmware updates to address security vulnerabilities.

https://www.dell.com/support/home/en-us/product-support/product/xps-15-9570-laptop/drivers

**HP DragonFly G2**

**Version: 01.08.20 Rev.A**

Fixes an issue where the system does not boot properly after switching between two different saved boot stores. - Addresses security vulnerabilities CVE-2022-23924, CVE-2022-23925, CVE-2022-23926, CVE-2022-23927, CVE-2022-23928, CVE-2022-23929, CVE-2022-23930, CVE-2022-23931, CVE-2022-23932, CVE-2022-23933, CVE-2022-23934. - Addresses security vulnerabilities CVE-2022-23953, CVE-2022-23954, CVE-2022-23955, CVE-2022-23956, CVE-2022-23957, CVE-2022-23958. - Adds a feature to control the display of the BIOS Admin login based on the setting, BIOS Administrator visible at power-on authentication, when Enhanced BIOS Authentication Mode (EBAM) is set. - Provides the following firmware: DisplayLink PXE UEFI Driver, version1.1.4 Embedded Controller (EC), version 37.2A.00 Intel GOP, version 17.0.1055 Intel Management Engine, version 15.0.35.1951 Intel Thunderbolt Firmware, version 14.0.0.4301 Realtek PXE UEFI Driver, version2.035 USB Type-C Power Delivery (PD) Firmware, version 7.5.0

https://support.hp.com/us-en/drivers/selfservice/swdetails/hp-elite-dragonfly-g2-notebook-pc/34514046/model/38455668/swItemId/ob-286953-1

# BIOS Updates – This is why YOU SHOULD CARE

## Lenovo X1

UEFI: 1.34 / ECP: 1.09- [Important] Update includes a security fix.

UEFI: 1.33 / ECP: 1.09

- [Important] Update includes a security fix.

UEFI: 1.32 / ECP: 1.09

- [Important] Address CVE-2020-0543. (https://cve.mitre.org//cgi-bin//cvename.cgi?name=CVE-2020-0543)
- [Important] Update includes a security fix.
- [Important] Addresses CVE-2019-6173 and CVE-2019-6196.
(https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-6173)
(https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-6196)

Refer to Lenovo's Security Advisory page for additional information about

LEN-27431 "DLL Search Path and Symbolic Link Vulnerabilities".
(https://support.lenovo.com/us/en/product_security/LEN-27431)

Vulnerabilities exploitable only during installation.
Previously installed version is not vulnerable to these CVEs.
https://download.lenovo.com/pccbbs/mobiles/n14uj32w.txt

## Microsoft Surface Laptop 4

The following update is available for Surface Laptop 4 with Intel Processor devices running Windows 10 October 2020 Update, version 20H2, or greater.

This update: Addresses critical security vulnerability and improves system stability.

Surface - Firmware - 10.7.141.0
Surface UEFI - Firmware

10.7.141.0

Addresses critical security vulnerability and improves system stability.

Surface - Firmware - 15.0.1680.1
Surface ME - Firmware

15.0.1680.1

Addresses critical security vulnerability and improves system stability.

https://support.microsoft.com/en-us/surface/surface- laptop-4-update-history-607537fa-c595-4797-9a2e-ee77015472f6

SO YOU ARE TELLING ME THAT I NEED TO **UPDATE** MY BIOS..

# BIOS Automation – Vendor Tools

Most manufactures offer some level of BIOS management software, if your manufacture of choice doesn't.. **Change your supplier**.. Here are some of the more well-known ones;

**Dell Command Update**

- https://www.dell.com/support/article/ie/en/iebsdt1/sln311129/dell-command-update?lang=en

**Lenovo**

- ThinkPad Update Script - PowerShell
  https://thinkdeploy.blogspot.com/2019/02/dynamically-updating-thinkpad-bios-from.html

**HP**

- System Software Manager - https://ftp.hp.com/pub/caps-softpaq/cmit/HP_SSM.html
- Bios Configuration Utility- https://ftp.hp.com/pub/caps-softpaq/cmit/HP_BCU.html

**Microsoft Surface Enterprise Manage Mode***

- https://docs.microsoft.com/en-us/surface/surface-enterprise-management-mode

# BIOS Automation – Vendor Specific Notes

- **Lenovo**
  - ThinkPads and ThinkStations support a restart
  - ThinkCentre require a shutdown with the exception of the latest generation
  - Supervisor password needs to be set physically
  - Updating BIOS in a 64-bit WinPE environment may cause an error – KB https://support.lenovo.com/ie/en/solutions/ht506076
- **HP**
  - Client Management Script Library
  - Automate BIOS upgrades, obtain compatible softpaqs & more
  - https://ftp.hp.com/pub/caps-softpaq/cmit/hp-cmsl.html

# BIOS Automation – PowerShell (DIY)

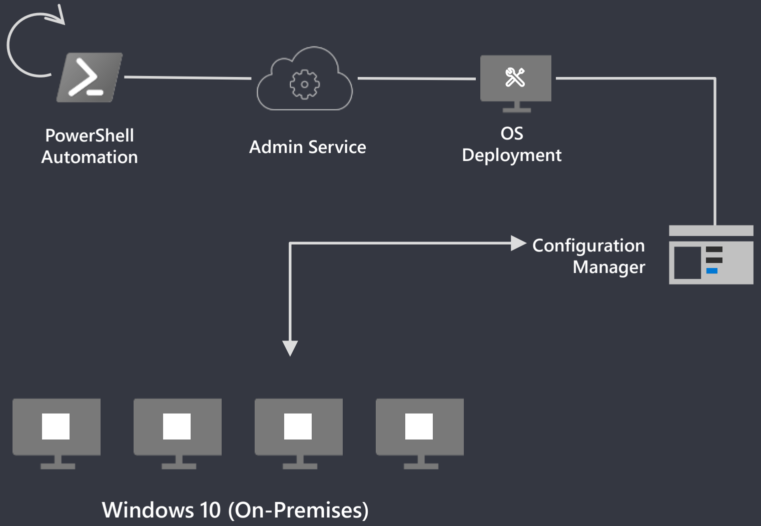
- If you can script it.. You can automate it
  - **Stop making excuses** not to learn PowerShell

# The Challenge We Face Today

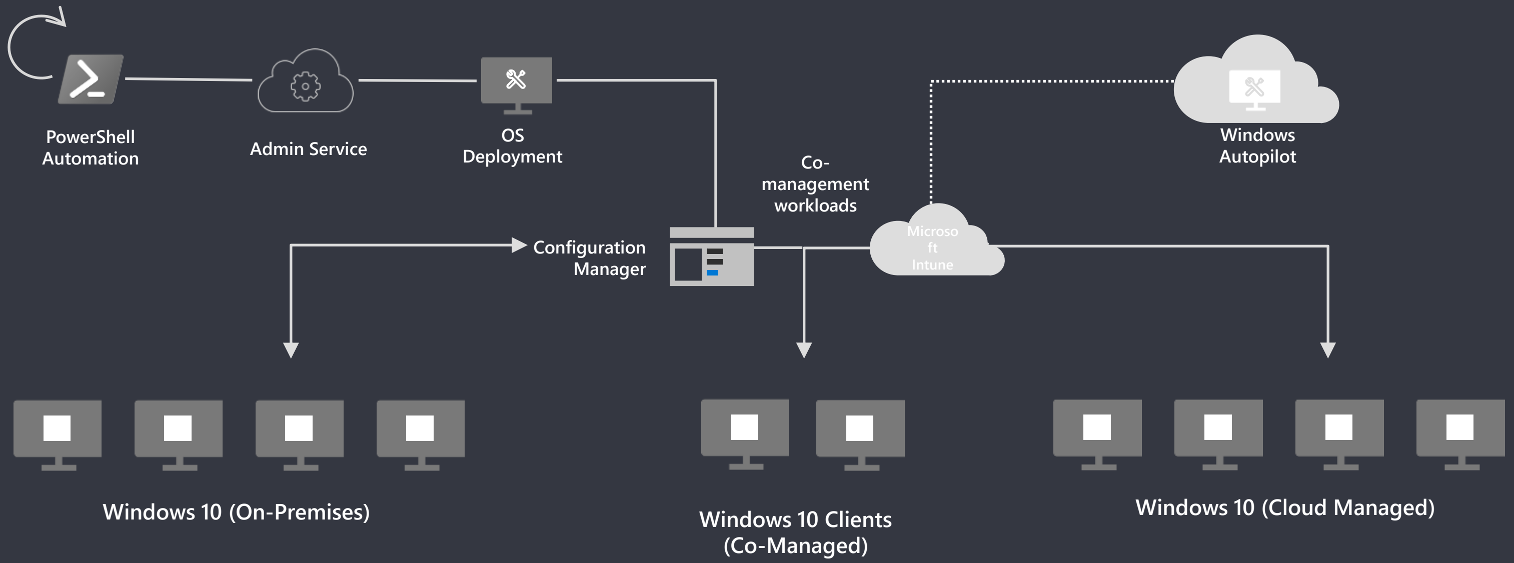
- Organisations have made big shifts in the way they manage devices
  - Home workers are now the norm
  - The desire to use Intune managed devices has seen massive growth due to this
- IT departments which to maintain the status quo
  - Provide the business with like for like functionality
  - Automate as much as possible
  - Port existing automation processes as much as possible

# Traditional OSD Overview

- **OS Deployment**
  - Traditional method
  - Admin Service
  - Custom Web Service
  - Custom Front Ends
  - PowerShell
- **Post OS Maintenance**
  - PowerShell
  - OEM Software

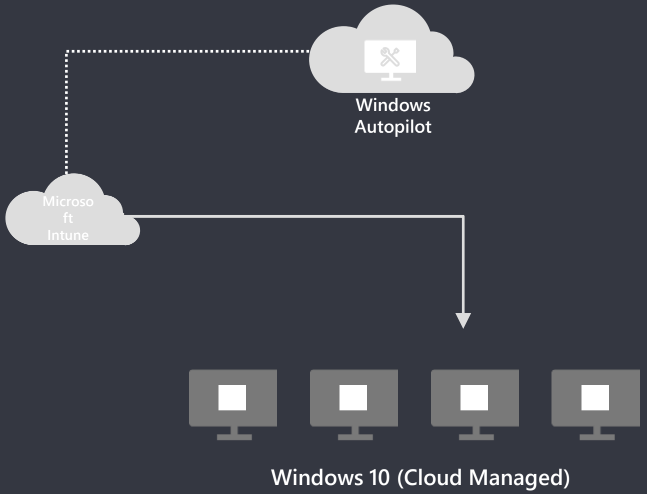


# Traditional Processes vs Modern Processes



# Intune Management Overview

- Windows Autopilot
  - Win32 Apps
  - PowerShell
- Post Deployment
  - How to control driver and firmware updates post provisioning?
  - OEM tools to the rescue..



nicX edition

# Demo BIOS Update Compliance

# OEM Solutions for Intune devices

Most OEM’s provide solutions, not all are equal

Microsoft

Built in support for driver and firmware updates through WUfB

Lenovo

Lenovo System Update

DELL

Dell Command Update

hp

HP Tech Pulse | CMSL HP Connect for MEM

# HP Solutions for Intune devices

## HP Client Management Script Library

How to do things the right way

- Install the CMSL from the PowerShell Gallery
  - Install-Module –Name HPCMSL*

    The NuGet Package Provider needs to be updated
    The PowerShellGet module needs to be updated

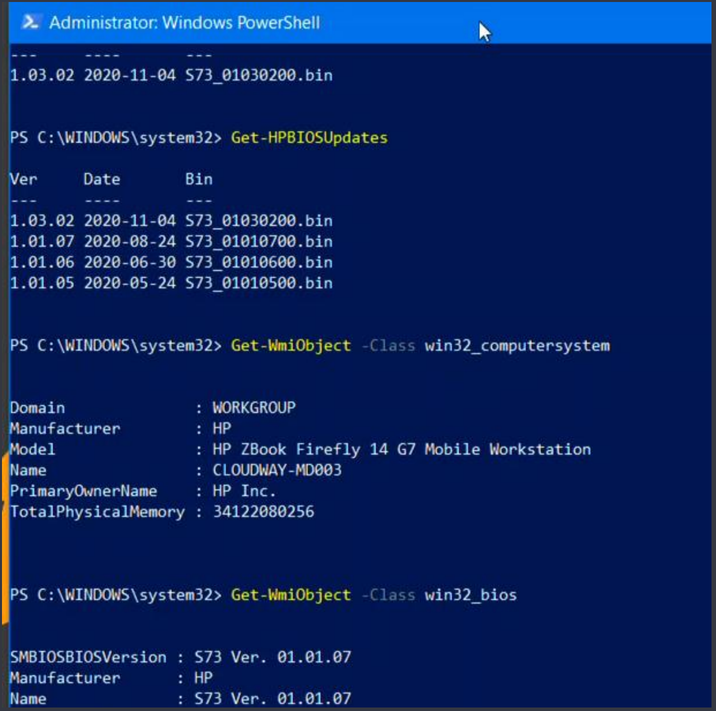
  - Automate driver and BIOS updates via PowerShell
    This sounds a bit more familiar

**HP CMSL PowerShell Module**

# Building an OEM scripted solution

- Upgrade the HP BIOS
  - Simple..

  - Get-HPBIOSUpdates
    - List all available updates
  - Get-HPBIOSUpdates –Flash
    - Update system to the latest BIOS release
  - Get-HPWindowsBIOSUpdate
  - Get-HPSoftPaq –Install
    - Download, extract, and install the latest drivers



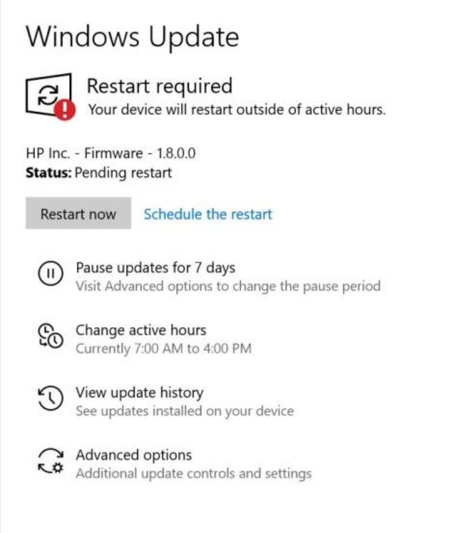
```
---     ----       ---
1.03.02 2020-11-04 S73_01030200.bin


PS C:\WINDOWS\system32> Get-HPBIOSUpdates

Ver     Date       Bin
---     ----       ---
1.03.02 2020-11-04 S73_01030200.bin
1.01.07 2020-08-24 S73_01010700.bin
1.01.06 2020-06-30 S73_01010600.bin
1.01.05 2020-05-24 S73_01010500.bin


PS C:\WINDOWS\system32> Get-WmiObject -Class win32_computersystem


Domain              : WORKGROUP
Manufacturer        : HP
Model               : HP ZBook Firefly 14 G7 Mobile Workstation
Name                : CLOUDWAY-MD003
PrimaryOwnerName    : HP Inc.
TotalPhysicalMemory : 34122080256



PS C:\WINDOWS\system32> Get-WmiObject -Class win32_bios


SMBIOSBIOSVersion : S73 Ver. 01.01.07
Manufacturer      : HP
Name              : S73 Ver. 01.01.07
```

# Updates over Windows Update

## HP Firmware Updates over Windows Update

- **Support for firmware updates through the normal update process**
- Leverages a mechanism built into the Unified Extensible Firmware Interface (UEFI) standard called UEFI Capsule
- **Worried? Need to disable this?**

  *Set-HPBIOSSettingValue -Name "Native OS Firmware Update Service" -Value “Disable"*



Windows Update

Restart required

Your device will restart outside of active hours.

HP Inc. - Firmware - 1.8.0.0

**Status:** Pending restart

Pause updates for 7 days

Visit Advanced options to change the pause period

Change active hours

Currently 7:00 AM to 4:00 PM

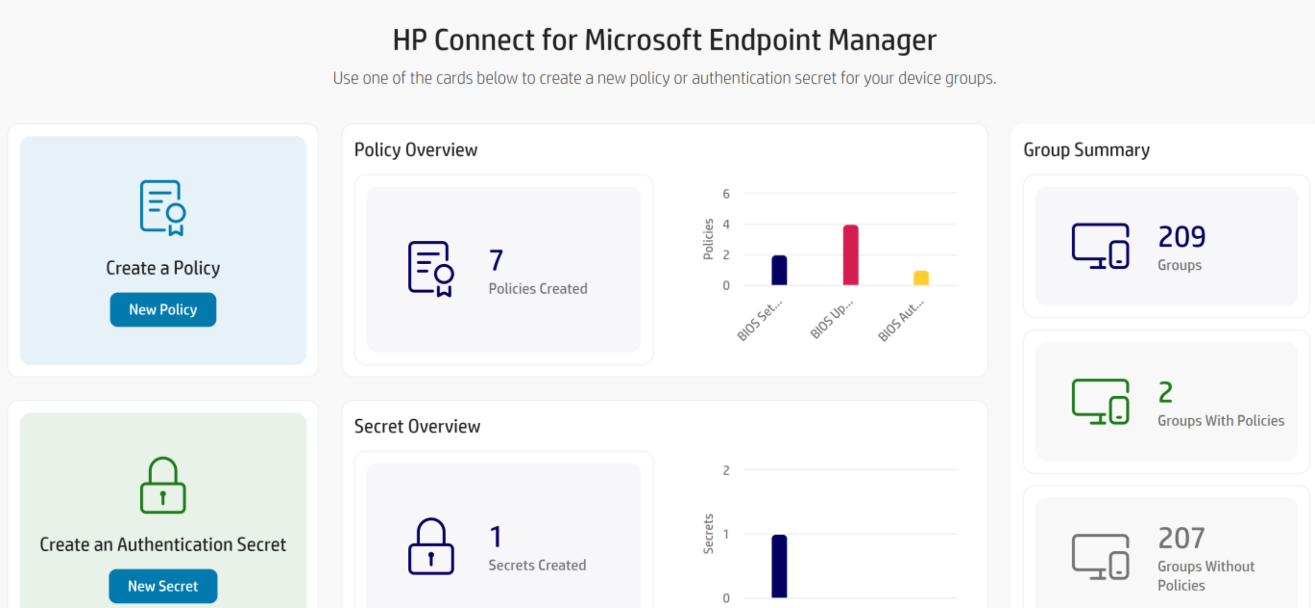
View update history

See updates installed on your device

Advanced options

Additional update controls and settings

# HP Connect for Microsoft Endpoint Manager



## HP Connect for Microsoft Endpoint Manager

Use one of the cards below to create a new policy or authentication secret for your device groups.

Create a Policy

New Policy

Create an Authentication Secret

New Secret

### Policy Overview

7
Policies Created

### Secret Overview

1
Secrets Created

### Group Summary

209
Groups

2
Groups With Policies

207
Groups Without Policies

https://admin.hp.com/

# Microsoft Native Improvements – Coming Soon

Microsoft deployment service for driver and firmware updates

# Proceed with Caution

# Control Is Good

BIOS & Firmware updates can have undesired results

- Administrative Control / Phased Upgrades
  - Providing a controlled method for testing upgrades is key to many organizations
  - It verifies stability prior to mass deployment
  - Consistent experience as we have today with Configuration Manager

# Intune BIOS Control – Our Thinking

Community Solution – Modern BIOS Management v2.0

- Driver Automation Tool creates a control file with approved BIOS release details
- Leverage OEM PS modules, in conjunction with control file for version control
- User Toast Notification prompts

# Demo

# BIOS Automation – Community Tools

## MSEndpointMgr.com – Modern BIOS Management

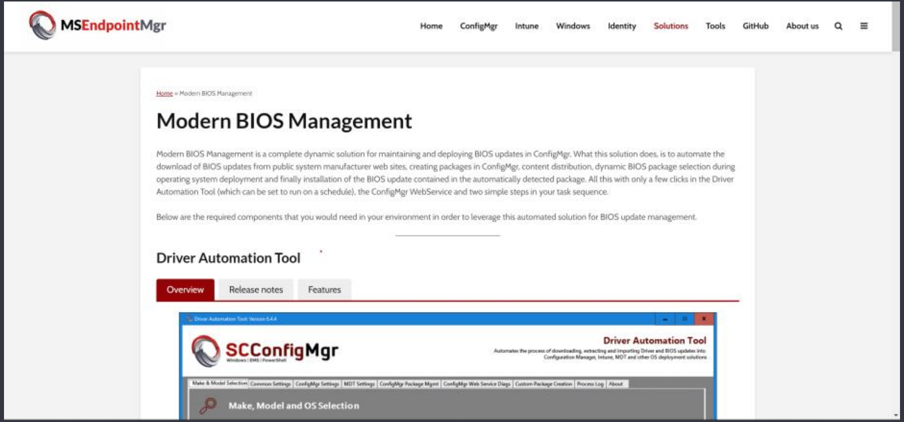
Developed by Maurice Daly and Nickolaj Andersen for use with Configuration Manager. With special thanks to individuals in Dell, Lenovo and HP for providing XML feeds and information.

### Full Automation Process

Supports Dell, HP & Lenovo

Three Step Process:

1. Download content & package (contains matching meta data)
2. Match model during TS
3. Apply BIOS with manufacturer specific script



Modern BIOS Management

Modern BIOS Management is a complete dynamic solution for maintaining and deploying BIOS updates in ConfigMgr. What this solution does, is to automate the download of BIOS updates from public system manufacturer web sites, creating packages in ConfigMgr, content distribution, dynamic BIOS package selection during operating system deployment and finally installation of the BIOS update contained in the automatically detected package. All this with only a few clicks in the Driver Automation Tool (which can be set to run on a schedule), the ConfigMgr WebService and two simple steps in your task sequence.

Below are the required components that you would need in your environment in order to leverage this automated solution for BIOS update management.

Driver Automation Tool

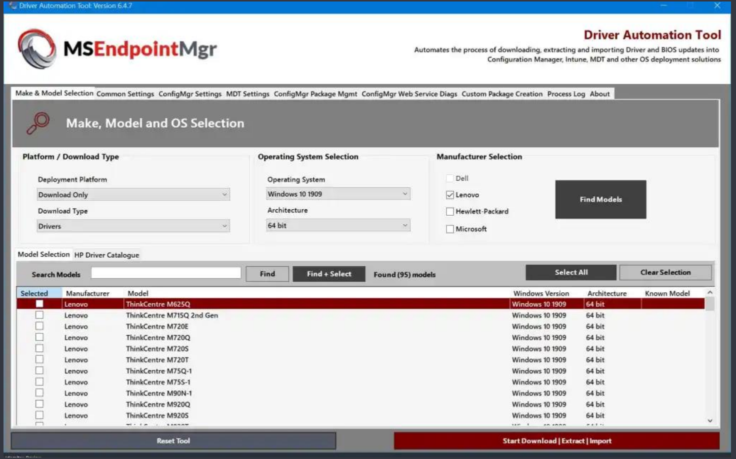
Overview
Release notes
Features
Driver Automation Tool Version 6.4.4
SCConfigMgr
Windows | EMS | PowerShell
Driver Automation Tool
Automates the process of downloading, extracting and importing Driver and BIOS updates into Configuration Manager, Intune, MDT and other OS deployment solutions
Make & Model Selection
Common Settings
ConfigMgr Settings
MDT Settings
ConfigMgr Package Mgmt
ConfigMgr Web Service Diags
Custom Package Creation
Process Log
About
Make, Model and OS Selection

# BIOS Automation – Community Tools

## MSEndpointMgr.com – Modern Driver Management

### Driver Automation Tool

https://github.com/maurice-daly/DriverAutomationTool



Driver Automation Tool: Version 6.4.7

MSEndpointMgr

Driver Automation Tool

Automates the process of downloading, extracting and importing Driver and BIOS updates into Configuration Manager, Intune, MDT and other OS deployment solutions

Make, Model and OS Selection

Platform / Download Type

Deployment Platform: Download Only

Download Type: Drivers

Operating System Selection

Operating System: Windows 10 1909

Architecture: 64 bit

Manufacturer Selection

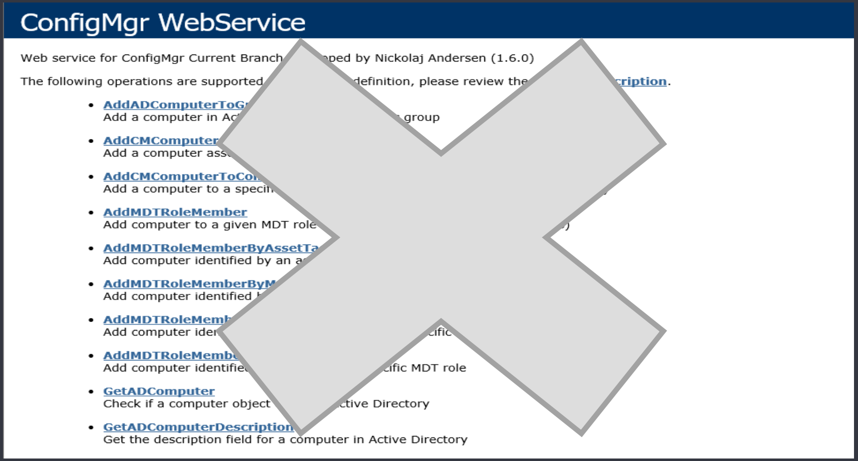
□ Dell
☑ Lenovo
□ Hewlett-Packard
□ Microsoft

Found (95) models

| Selected | Manufacturer | Model | Windows Version | Architecture | Known Model |
|---|---|---|---|---|---|
| □ | Lenovo | ThinkCentre M625Q | Windows 10 1909 | 64 bit | |
| □ | Lenovo | ThinkCentre M715Q 2nd Gen | Windows 10 1909 | 64 bit | |
| □ | Lenovo | ThinkCentre M720E | Windows 10 1909 | 64 bit | |
| □ | Lenovo | ThinkCentre M720Q | Windows 10 1909 | 64 bit | |
| □ | Lenovo | ThinkCentre M720S | Windows 10 1909 | 64 bit | |
| □ | Lenovo | ThinkCentre M720T | Windows 10 1909 | 64 bit | |
| □ | Lenovo | ThinkCentre M75Q-1 | Windows 10 1909 | 64 bit | |
| □ | Lenovo | ThinkCentre M75S-1 | Windows 10 1909 | 64 bit | |
| □ | Lenovo | ThinkCentre M90N-1 | Windows 10 1909 | 64 bit | |
| □ | Lenovo | ThinkCentre M920Q | Windows 10 1909 | 64 bit | |
| □ | Lenovo | ThinkCentre M920S | Windows 10 1909 | 64 bit | |

### ConfigMgr WebService

https://gallery.technet.microsoft.com/ConfigMgr-WebService-100-572825b2



ConfigMgr WebService

Web service for ConfigMgr Current Branch ped by Nickolaj Andersen (1.6.0)

The following operations are supported definition, please review the cription.

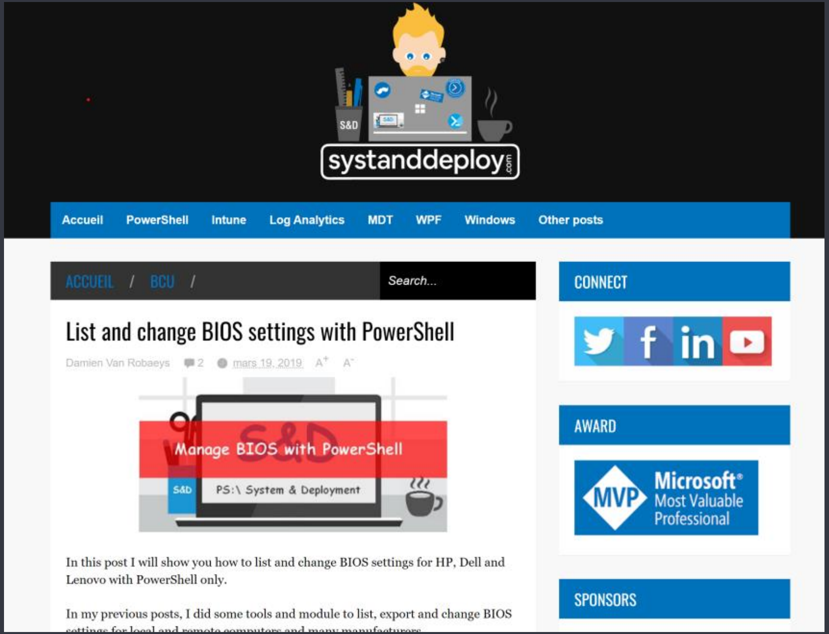
- AddADComputerToG
  Add a computer in Ac group
- AddCMComputer
  Add a computer ass
- AddCMComputerToCo
  Add a computer to a specifi
- AddMDTRoleMember
  Add computer to a given MDT role )
- AddMDTRoleMemberByAssetTa
  Add computer identified by an a
- AddMDTRoleMemberByM
  Add computer identified b
- AddMDTRoleMemb
  Add computer ider cific
- AddMDTRoleMemb
  Add computer identifie cific MDT role
- GetADComputer
  Check if a computer object ctive Directory
- GetADComputerDescription
  Get the description field for a computer in Active Directory

# BIOS Automation – Community Tools

**Damien Van Robaeys**

BIOS settings management for Dell, HP, and Lenovo

List and change BIOS settings with PowerShell | Syst & Deploy (systanddeploy.com)



List and change BIOS settings with PowerShell

Damien Van Robaeys 2 mars 19, 2019 A+ A-

In this post I will show you how to list and change BIOS settings for HP, Dell and Lenovo with PowerShell only.

In my previous posts, I did some tools and module to list, export and change BIOS settings for local and remote computers and many manufacturers.

Slides and demos from the conference will be available at

**https://github.com/nordicinfrastructureconference/2022**