|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Benämning** | OVB - 180705 | Ansvarig | Claes Gyllhamn | Skapat | 2018-07-05 10:42 |
| **Projekt** | Omvärldsbevakning | | | Senast sparat | 2018-07-06 15:18 |
| **Revision** | 0.1 | Filnamn | OVB\_180705.docx | | |

Omvärldsbevakning

(kund)

Innehåll

[1 Veckovis kontroll 3](#_Toc518567051)

[1.1 Comex KT2 3](#_Toc518567052)

[1.1.1 Versionsnivå 3](#_Toc518567053)

[1.1.2 Sårbarhet 3](#_Toc518567054)

[1.2 Dell PowerEdge R220 3](#_Toc518567055)

[1.2.1 Versionsnivå 3](#_Toc518567056)

[1.2.2 Sårbarhet 3](#_Toc518567057)

[1.3 Dell PowerEdge R630 3](#_Toc518567058)

[1.3.1 Versionsnivå 3](#_Toc518567059)

[1.3.2 Sårbarhet 4](#_Toc518567060)

[1.4 Fibersystem 50-807 4](#_Toc518567061)

[1.4.1 Versionsnivå 4](#_Toc518567062)

[1.4.2 Sårbarhet 4](#_Toc518567063)

[1.5 Microsoft Windows ThinPC 7 4](#_Toc518567064)

[1.5.1 Versionsnivå 4](#_Toc518567065)

[1.5.2 Sårbarheter 4](#_Toc518567066)

[2 Summering 4](#_Toc518567067)

[3 Beskrivning av kontroller 4](#_Toc518567068)

[3.1 Hård & mjukvara 4](#_Toc518567069)

# Hårdvara Veckovis kontroll

Då det inte kommer ut CVE eller andra definitioner av sårbarhet lika ofta som till t.ex. mjukvara så blir det desto mer manuellt arbete för att få fram den information som önskas för hårdvara. När det gäller mjukvara finns det ofta definitioner på sidor så som <https://www.cvedetails.com/index.php> vilket gör att information är lite mer lättillgänglig.

## Comex KT2

Länk: <http://www.comex.se/index.php/sv/produkter/forsvar/datasakerhet/comex-biosec-reader>

### Versionsnivå

Nuvarande nivå av hårdvara ser ut att vara den som fortsatt kommer nyttjas, därför finns ingen rekommendation här.

### Sårbarhet

Inga sårbarheter funna vid traditionell sökning.

## Dell NX3220

Länk:

### Versionsnivå

Blabla

### Sårbarhet

Blabla

## Dell PowerEdge R220

Länk: <http://www.dell.com/se/foretag/p/poweredge-r220/pd>

### Versionsnivå

Rekommendation från tillverkare, uppdatera till PowerEdge R230 då R220 inte längre finns till för försäljning. **[OBS, rekommendation från tillverkare]**.

### Sårbarhet

**Åtgärd behöver vidtas.**

Kan vara sårbar mot Spectre/Meltdown utifall uppdatering inte genomförts.

Länk: <https://www.vulnerabilitycenter.com/#!vul=80043>

## Dell PowerEdge R630

Länk: <http://www.dell.com/se/foretag/p/poweredge-r630/pd>

### Versionsnivå

Version är OK, ingen rekommendation om uppgradering.

### Sårbarhet

**Åtgärd behöver vidtas.**

Kan vara sårbar mot Spectre/Meltdown utifall uppdatering inte genomförts.

Länk: <https://www.vulnerabilitycenter.com/#!vul=80043>

## Fibersystem 50-807

Länk:

<https://www.fibersystem.com/product/fiber-optical-converter-extender-12-port-100basetx-to-100basefx-mm-sc-50-807/>

### Versionsnivå

Version är OK.

### Sårbarhet

Inga sårbarheter funna vid traditionell sökning

## Fibersystem 50-50004B

Länk:

<https://www.fibersystem.com/product/card-module-1000baset-1000basesx-lx-lc-50-50004/>

### Versionsnivå

Version är OK.

### Sårbarhet

Inga sårbarheter funna vid traditionell sökning

## Fibersystem 60-005891

Länk:

Ingen information funnen

### Versionsnivå

Vet ej

### Sårbarhet

Ingen information funnen

## Fibersystem B10

Länk:

Ingen information funnen

### Versionsnivå

Vet ej

### Sårbarhet

Ingen information funnen

## Fibersystem B11

Länk:

Ingen information funnen

### Versionsnivå

Vet ej

### Sårbarhet

Ingen information funnen

## Cisco 2951/K9

Länk:

<https://www.cisco.com/c/en/us/support/routers/2951-integrated-services-router-isr/model.html>

### Versionsnivå

End of sale: 2017

End of support: 2022-12-31 , bör bytas ut innan dess.

Beroende på moduler som nyttjas så kan t.ex. vissa chip bli överhettade. Cisco har gått ut och informerat samt kört ett utbytesprogram för att hantera detta problem.  
<https://www.cisco.com/c/en/us/support/docs/field-notices/640/fn64096.html>

Beroende på ROMMON version som nyttjas, så kan det bli problem vid RJ45/Console anslutning och att skicka ”BREAK” kommando (vilket nyttjas vid lösenordsåterställning bland annat).

<https://www.cisco.com/c/en/us/support/docs/field-notices/633/fn63355.html>

### Sårbarhet

Ingen information rörande sårbarhet i hårdvara, IOS är den attackvektor som brukar nyttjas.

## Cisco UCS-E140S-M1

Länk:

<https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-e-series-servers/datasheet-c78-737705.html> ytterligare information kräver partnernivå hos Cisco.

### Versionsnivå

End of sale: 2016

End of support: 2021-03-31 , bör bytas ut innan dess.

<https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-e-series-servers/eos-eol-notice-c51-735780.html>

### Sårbarhet

Beroende på version av BIOS och IOS XE som nyttjas så finns det en del hårdvarurelaterade buggar/sårbarheter.

Exempel enligt:

<https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/e/3-1-1/release/notes/3_1_1_release_notes.html>

<https://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-20180620-encs-ucs-bios-auth-bypass.html>

## Cisco Catalyst 3650-24TS-S

Länk: <https://www.cisco.com/c/en/us/support/switches/catalyst-3650-24ts-s-switch/model.html>

### Versionsnivå

End of sale: Inget annonserat

End of support: Inget annonserat

Version anses OK av hårdvara.

om det är en 3650V2 bör den migreras till: <https://www.cisco.com/c/en/us/products/switches/catalyst-3650-series-switches/index.html>

### Sårbarhet

Funna sårbarheter rör det OS som switch nyttjar.

## Cisco SM-ES3-24-P

Länk: <https://www.cisco.com/c/en/us/support/interfaces-modules/enhanced-layer-2-3-etherswitch-service-module/model.html?dtid=osscdc000283#End-of-LifeandEnd-of-SaleNotices>

### Versionsnivå

End of sale: Inget annonserat

End of support: Inget annonserat

Version anses OK av hårdvara.

### Sårbarhet

Funna sårbarheter rör det OS som switchmodul nyttjar.

## Cisco SM-ES3-24-P

Länk: <https://www.cisco.com/c/en/us/support/interfaces-modules/enhanced-layer-2-3-etherswitch-service-module/model.html?dtid=osscdc000283#End-of-LifeandEnd-of-SaleNotices>

### Versionsnivå

End of sale: Inget annonserat

End of support: Inget annonserat

Version anses OK av hårdvara.

### Sårbarhet

Funna sårbarheter rör det OS som switchmodul nyttjar.

## Advenica SecuriVPN arana 9301B

Länk: <https://www.cisco.com/c/en/us/support/interfaces-modules/enhanced-layer-2-3-etherswitch-service-module/model.html?dtid=osscdc000283#End-of-LifeandEnd-of-SaleNotices>

### Versionsnivå

Version anses OK av hårdvara, för ytterligare information om tillgängliga modeller och rekommendationer behövs kontakt med Advenica.

### Sårbarhet

Inga sårbarheter funna vid traditionell sökning

# Mjukvara veckovis kontroll

## Microsoft Windows ThinPC 7

### Versionsnivå

Windows Thin PC ligger i “Extended support” kategorin, vilket innebär att då support för Windows 7 upphör under 2020 så kommer även Thin PC 7 drabbas. Ersättningsalternativ bör utvärderas i god tid innan.

### Sårbarheter

Inga sårbarheter funna vid traditionell sölning

## Microsoft Windows ThinPC 7

### Versionsnivå

Windows Thin PC ligger i “Extended support” kategorin, vilket innebär att då support för Windows 7 upphör under 2020 så kommer även Thin PC 7 drabbas. Ersättningsalternativ bör utvärderas i god tid innan.

### Sårbarheter

Inga sårbarheter funna vid traditionell sölning

# Summering

## test

Firmware behöver verifieras på enheter nedan för att verifiera så de ej är sårbara.

* Dell PowerEdge R220
* Dell PowerEdge R630

# Beskrivning av kontroller

## Hård & mjukvara

|  |  |  |
| --- | --- | --- |
| **Funktion** | **Kontroll** | **Verktyg** |
| Hårdvara | Version & sårbarhet | Manuellt (google, tillverkares hemsida, cve-details och liknande) |
| Mjukvara | Version & sårbarhet | Manuellt och delvis automatiserat. Liknande metoder som för hårdvara. |