|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **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\_v0.1.docx | | |

Omvärldsbevakning

(kund)

Innehåll

[1 Hårdvara Veckovis kontroll 6](#_Toc518916862)

[1.1 Comex KT2 6](#_Toc518916863)

[1.1.1 Versionsnivå 6](#_Toc518916864)

[1.1.1 Sårbarhet 6](#_Toc518916865)

[1.2 Dell NX3220 6](#_Toc518916866)

[1.2.1 Versionsnivå 6](#_Toc518916867)

[1.2.2 Sårbarhet 6](#_Toc518916868)

[1.2 Dell PowerEdge R220 6](#_Toc518916869)

[1.2.1 Versionsnivå 6](#_Toc518916870)

[1.2.2 Sårbarhet 6](#_Toc518916871)

[1.3 Dell PowerEdge R630 7](#_Toc518916872)

[1.3.1 Versionsnivå 7](#_Toc518916873)

[1.3.2 Sårbarhet 7](#_Toc518916874)

[1.4 Fibersystem 50-807 7](#_Toc518916875)

[1.4.1 Versionsnivå 7](#_Toc518916876)

[1.4.2 Sårbarhet 7](#_Toc518916877)

[1.5 Fibersystem 50-50004B 7](#_Toc518916878)

[1.5.1 Versionsnivå 7](#_Toc518916879)

[1.5.2 Sårbarhet 7](#_Toc518916880)

[1.6 Fibersystem 60-005891 7](#_Toc518916881)

[1.6.1 Versionsnivå 7](#_Toc518916882)

[1.6.2 Sårbarhet 7](#_Toc518916883)

[1.7 Fibersystem B10 8](#_Toc518916884)

[1.7.1 Versionsnivå 8](#_Toc518916885)

[1.7.2 Sårbarhet 8](#_Toc518916886)

[1.8 Fibersystem B11 8](#_Toc518916887)

[1.8.1 Versionsnivå 8](#_Toc518916888)

[1.8.2 Sårbarhet 8](#_Toc518916889)

[1.9 Cisco 2951/K9 8](#_Toc518916890)

[1.9.1 Versionsnivå 8](#_Toc518916891)

[1.9.2 Sårbarhet 8](#_Toc518916892)

[1.10 Cisco UCS-E140S-M1 9](#_Toc518916893)

[1.10.1 Versionsnivå 9](#_Toc518916894)

[1.10.2 Sårbarhet 9](#_Toc518916895)

[1.11 Cisco Catalyst 3650-24TS-S 9](#_Toc518916896)

[1.11.1 Versionsnivå 9](#_Toc518916897)

[1.11.2 Sårbarhet 9](#_Toc518916898)

[1.12 Cisco SM-ES3-24-P 9](#_Toc518916899)

[1.12.1 Versionsnivå 9](#_Toc518916900)

[1.12.2 Sårbarhet 10](#_Toc518916901)

[1.13 Cisco SM-ES3-24-P 10](#_Toc518916902)

[1.13.1 Versionsnivå 10](#_Toc518916903)

[1.13.2 Sårbarhet 10](#_Toc518916904)

[1.14 Advenica SecuriVPN arana 9301B 10](#_Toc518916905)

[1.14.1 Versionsnivå 10](#_Toc518916906)

[1.14.2 Sårbarhet 10](#_Toc518916907)

[2 Mjukvara veckovis kontroll 10](#_Toc518916908)

[2.1 Microsoft Windows ThinPC 7 10](#_Toc518916909)

[2.1.1 Versionsnivå 10](#_Toc518916910)

[2.1.2 Sårbarheter 11](#_Toc518916911)

[2.2 Microsoft Office 2010 11](#_Toc518916912)

[2.2.1 Versionsnivå 11](#_Toc518916913)

[2.2.2 Sårbarheter 11](#_Toc518916914)

[2.3 .NET 4.6 11](#_Toc518916915)

[2.3.1 Versionsnivå 11](#_Toc518916916)

[2.3.2 Sårbarheter 11](#_Toc518916917)

[2.4 Visual C++ Runtime (2005-2013) 11](#_Toc518916918)

[2.4.1 Versionsnivå 11](#_Toc518916919)

[2.4.2 Sårbarheter 11](#_Toc518916920)

[2.5 Microsoft Windows Server 2012 R2 11](#_Toc518916921)

[2.5.1 Versionsnivå 11](#_Toc518916922)

[2.5.2 Sårbarheter 11](#_Toc518916923)

[2.6 Citrix XenDesktop LTSR 7.6 12](#_Toc518916924)

[2.6.1 Versionsnivå 12](#_Toc518916925)

[2.6.2 Sårbarheter 12](#_Toc518916926)

[2.7 Citrix Receiver 4.3 12](#_Toc518916927)

[2.7.1 Versionsnivå 12](#_Toc518916928)

[2.7.2 Sårbarheter 12](#_Toc518916929)

[2.8 FoxIT Reader 7.2 12](#_Toc518916930)

[2.8.1 Versionsnivå 12](#_Toc518916931)

[2.8.2 Sårbarheter 12](#_Toc518916932)

[2.9 VMWare Tools 10.0 12](#_Toc518916933)

[2.9.1 Versionsnivå 12](#_Toc518916934)

[2.9.2 Sårbarheter 12](#_Toc518916935)

[2.10 VMWare ESXi 6.0 U1 12](#_Toc518916936)

[2.10.1 Versionsnivå 12](#_Toc518916937)

[2.10.2 Sårbarheter 13](#_Toc518916938)

[2.11 VMWare vSphere Client 6.o U1 13](#_Toc518916939)

[2.11.1 Versionsnivå 13](#_Toc518916940)

[2.11.2 Sårbarheter 13](#_Toc518916941)

[2.12 VMWare vCenter Server 6.0 U1 13](#_Toc518916942)

[2.12.1 Versionsnivå 13](#_Toc518916943)

[2.12.2 Sårbarheter 13](#_Toc518916944)

[2.13 Redhat Enterprise Linux 6.5 13](#_Toc518916945)

[2.13.1 Versionsnivå 13](#_Toc518916946)

[2.13.2 Sårbarheter 13](#_Toc518916947)

[2.14 Google Chrome 46 13](#_Toc518916948)

[2.14.1 Versionsnivå 13](#_Toc518916949)

[2.14.2 Sårbarheter 13](#_Toc518916950)

[2.15 Java Runtime 8 U65 13](#_Toc518916951)

[2.15.1 Versionsnivå 13](#_Toc518916952)

[2.15.2 Sårbarheter 14](#_Toc518916953)

[2.16 Cisco IOS-XE 3.6 14](#_Toc518916954)

[2.16.1 Versionsnivå 14](#_Toc518916955)

[2.16.2 Sårbarheter 14](#_Toc518916956)

[2.17 Cisco IOS 15.2 14](#_Toc518916957)

[2.17.1 Versionsnivå 14](#_Toc518916958)

[2.17.2 Sårbarheter 14](#_Toc518916959)

[2.18 FM Mallar 2010 14](#_Toc518916960)

[2.18.1 Versionsnivå 14](#_Toc518916961)

[2.18.2 Sårbarheter 14](#_Toc518916962)

[2.19 FM GrAST 1.4.6 14](#_Toc518916963)

[2.19.1 Versionsnivå 14](#_Toc518916964)

[2.19.2 Sårbarheter 14](#_Toc518916965)

[2.20 KrAPIc 3.2.3 14](#_Toc518916966)

[2.20.1 Versionsnivå 14](#_Toc518916967)

[2.20.2 Sårbarheter 15](#_Toc518916968)

[2.21 CUAP-L 3.1.0 15](#_Toc518916969)

[2.21.1 Versionsnivå 15](#_Toc518916970)

[2.21.2 Sårbarheter 15](#_Toc518916971)

[2.22 FM Tunnel 2.3.0 15](#_Toc518916972)

[2.22.1 Versionsnivå 15](#_Toc518916973)

[2.22.2 Sårbarheter 15](#_Toc518916974)

[2.23 FM NetFilter 2.3.0 15](#_Toc518916975)

[2.23.1 Versionsnivå 15](#_Toc518916976)

[2.23.2 Sårbarheter 15](#_Toc518916977)

[3 Summering 15](#_Toc518916978)

[3.1 Rekommendationer hårdvara 15](#_Toc518916979)

[3.2 Rekommendationer Mjukvara 16](#_Toc518916980)

[4 Beskrivning av kontroller 16](#_Toc518916981)

[4.1 Hård & mjukvara 16](#_Toc518916982)

# 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: <https://www.dell.com/en-us/work/shop/cty/powervault-nx3200-network-attached-storage/spd/powervault-nx3200>

### Versionsnivå

Ingen ytterligare information funnen om den specifika modellen.

### Sårbarhet

Inga sårbarheter funna vid traditionell sökning.

## 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

Under kontroll av mjukvara räknas ej äldre sårbarheter med då antagande görs att ett rullande patchningsschema redan finns på plats. Utifall en mer utförlig rapport önskas där äldre sårbarheter finns med, kontakta West Code Solutions AB.

Kontroll i skrivande stund sker från 2018-01-01 till aktuellt datum.

## 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 Office 2010

### Versionsnivå

Microsoft office 2010 är av den äldre varianten och möjligheter till uppdatering bör ses över.

### Sårbarheter

Det är många sårbarheter som dykt upp, se bifogad rapport för ytterligare information:

2018-07-09-result-office.html

## .NET 4.6

### Versionsnivå

.NET ramverket följer med windows och bör hållas på den senaste stabila nivån som behövande program klarar.

### Sårbarheter

En del sårbarheter funna, se bifogad rapport:

2018-07-09-result-.net\_framework.html

## Visual C++ Runtime (2005-2013)

### Versionsnivå

Verifiera att äldre versioner inte är exponerade utåt då de innehåller sårbarheter.

### Sårbarheter

2005: inga från i år

2008: inga från i år

2010: inga från i år

2012: inga från i år

2013: inga från i år

## Microsoft Windows Server 2012 R2

### Versionsnivå

Server 2012 R2 är fortfarande en OK version, utökad support räcker fram till 2023-10-10. Mainstream support upphör 2018-10-09

### Sårbarheter

Flertalet sårbarheter har dykt upp under året, se bifogad rapport:

2018-07-09-result-windows\_server\_2012.html

## Citrix XenDesktop LTSR 7.6

### Versionsnivå

Version 7.15 av Long Term Service Release finns tillgänglig. Översyn rörande uppgradering bör genomföras.

### Sårbarheter

Inga funna för i år vid traditionell sökning.

## Citrix Receiver 4.3

### Versionsnivå

Version 4.12 finns ute, vilket bör utvärderas.

### Sårbarheter

Inga funna för i år vid traditionell sökning.

## FoxIT Reader 7.2

### Versionsnivå

Version 9.1 finns ute och bör utvärderas.

### Sårbarheter

Ett par sårbarheter har dykt upp för i år, se bifogad rapport:

2018-07-09-result-foxit\_reader.html

## VMWare Tools 10.0

### Versionsnivå

Vmware tools och vm hardware bör uppgraderas i takt med att vmware ESXi uppgraderas. Så länge versionerna följer med varandra så är det OK.

### Sårbarheter

Inga funna för i år vid traditionell sökning.

## VMWare ESXi 6.0 U1

### Versionsnivå

Version 6.5 har funnits ute ett tag samt har ett par servicepacks, därför bör en uppgradering utvärderas.

### Sårbarheter

Inga nya sårbarheter har dykt upp ännu i år, däremot har några äldre fått uppdateringar. Vilket kan påverka flera versioner. Exempelvis: <https://www.cvedetails.com/cve/CVE-2017-4941/>

## VMWare vSphere Client 6.o U1

### Versionsnivå

Den ”feta” klienten kommer inte finnas kvar framöver, all administration av vcenter sker via webbgui istället. Något att ha i åtanke inför uppgradering och fortsatt administration.

### Sårbarheter

Inga funna för i år vd traditionell sökning

## VMWare vCenter Server 6.0 U1

### Versionsnivå

Denna bör uppgraderas i samband med att ESXi uppgraderas.

### Sårbarheter

Inga funna för i år vid traditionell sökning.

## Redhat Enterprise Linux 6.5

### Versionsnivå

Version 7 har varit ute ett tag samt fått ett par servicepacks, därför bör detta utvärderas. På grund av ny struktur rörande tjänster så är det något att ha i åtanke vid migrering (exempelvis SystemD istället för SystemV).

### Sårbarheter

Se bifogad rapport: 2018-07-09-result-enterprise\_linux.html

## Google Chrome 46

### Versionsnivå

Version 67 är senaste huvudversionen och bör utvärderas.

### Sårbarheter

Det finns rätt många sårbarheter för äldre versioner av chrome, varför en uppgradering är rekommenderad. Se bifogad rapport: 2018-07-09-result-chrome.html

## Java Runtime 8 U65

### Versionsnivå

Version 8 Update 171 är ute och bör utvärderas.

### Sårbarheter

Se bifogad rapport: 2018-07-09-result-jre.html

## Cisco IOS-XE 3.6

### Versionsnivå

Verifiering att 3.6 är senaste version & att rommon/bios är OK rekommenderas.

### Sårbarheter

Se bifogad rapport: 2018-07-09-result-ios\_xe.html

## Cisco IOS 15.2

### Versionsnivå

Beroende på switch/router som nyttjar IOS så finns det nyare versioner och dessa bör utvärderas.

### Sårbarheter

Se bifogad rapport: 2018-07-09-result-ios.html

## FM Mallar 2010

### Versionsnivå

Information saknas

### Sårbarheter

Information saknas

## FM GrAST 1.4.6

### Versionsnivå

Information saknas

### Sårbarheter

Information saknas

## KrAPIc 3.2.3

### Versionsnivå

Information saknas

### Sårbarheter

Information saknas

## CUAP-L 3.1.0

### Versionsnivå

Information saknas

### Sårbarheter

Information saknas

## FM Tunnel 2.3.0

### Versionsnivå

Information saknas

### Sårbarheter

Information saknas

## FM NetFilter 2.3.0

### Versionsnivå

Information saknas

### Sårbarheter

Information saknas

# Summering

## Rekommendationer hårdvara

Genomgång av BIOS samt Firmware på samtliga enheter för att verifiera så version är i linje med rekommendation från leverantör. Applicering av buggfixar är alltid rekommenderad för att bibehålla en stabilt miljö samt enhet.

## Rekommendationer Mjukvara

Då det finns nyare versioner och/eller patchar till många programvaror så är rekommendationen att dessa utvärderas för att se huruvida de bör uppgraderas.

# 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. |