



CyberArk 軟體安全要求 及漏洞更新建議

力悅資訊白皮書

1. 根據 CyberArk 原廠建議，CyberArk 軟體安裝或更新完成後，務必進行作業系統強化(Harden)，強化後的任何系統設定及作業系統漏洞更新作業，均須遵照 CyberArk 官方資安通報所提供的更新方法，進行軟體強化更新。（各經銷商煩請聯絡代理商力悅，協助提供更新軟體）

✓ Harden the Digital Vault Server operating system

The Digital Vault Server operating system must be hardened to the configuration and patch level supplied by CyberArk.

The Digital Vault application installation includes hardening of the operating system based on the Microsoft Security Compliance Manager (SCM) server hardening recommendations. During application installation, the operating system is further hardened with configurations to meet the specific needs of the Digital Vault software.

Because the Digital Vault Server is configured to serve only CyberArk protocol requests, the hardening process deactivates many operating system services that are not required for the operation of the Digital Vault application. As such, it will not function as a regular domain member in a Windows network.

Harden the CPM and PVWA Servers

This section describes automatic and manual procedures for hardening CyberArk's CPM and PVWA servers. These procedures were tested and reviewed by CyberArk's Research and Development department and CyberArk's Security Team. The automatic procedure and the manual procedure complement each other and, therefore, both must be applied.

When the CPM and PVWA server environments are part of Active Directory domain ('In Domain'), the automatic hardening procedure is based on a prepared GPO (Group Policy Object) file. However, when the CPM and PVWA server environments are not a part of Active Directory domain ('Out of Domain'), it is based on an INF file.

This section describes how to harden CyberArk's CPM and PVWA servers that are installed on Windows 2012R2 and Windows 2016 Servers in 'In Domain' deployments as well as in 'Out of Domain' deployments.

詳細資訊請參考以下網址：

<https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/11.2/en/Content/Security/CyberArk-DV-Server-Security-Standards-Requirements.htm>

2. 常見的企業級資安解決方案，與 CyberArk 軟體可能產生嚴重衝突，

故應 嚴格禁止 執行以下列舉之軟體行為：

- 在數位金庫上安裝防毒軟體
- 在數位金庫上安裝監控軟體
- 在數位金庫上安裝備份與還原軟體
- 對 CyberArk 軟體進行定期的作業系統更新及漏洞修補更新作業

Various enterprise solutions may conflict with the CyberArk Digital Vault Security Standard and customers might inadvertently create risk by not conforming to the standard.

- > Anti-virus software on the Digital Vault Server
- > Monitoring software on the Digital Vault Server
- > Backup and recovery software on the Digital Vault Server.
- ✓ Microsoft updates and patches to be applied monthly

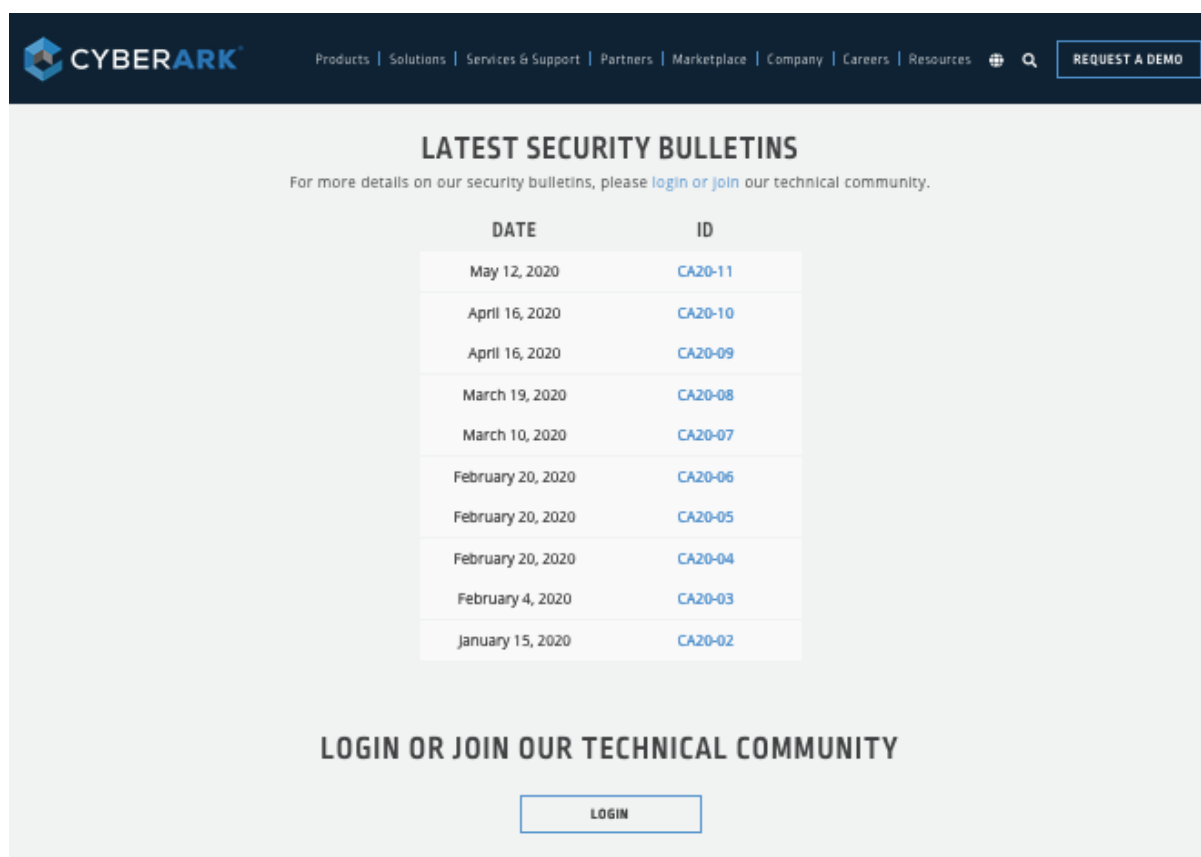
As a standard practice, many organizations requires Windows servers to be patched on a monthly basis.

Every Microsoft patch for relevant operating systems is reviewed by the CyberArk Security Team. When a patch is deemed necessary, CyberArk notifies customers, and the CyberArk Support Team is available to assist. With the greatly reduced attack surface of a standard-conforming Digital Vault Server, a vast majority of patches released are not required.

詳細資訊請參考以下網址：

<https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/11.2/en/Content/Security/Standards-Handling%20Exceptions.htm>

3. CyberArk 原廠會針對所有微軟公司所發佈的作業系統更新進行分析，若有需要針對 CyberArk 系統進行更新的資安更新作業，會即時公佈在官方所提供的資安公報網站上，並且會主動通知客戶進行系統強化。



CYBERARK Products | Solutions | Services & Support | Partners | Marketplace | Company | Careers | Resources

LATEST SECURITY BULLETINS

For more details on our security bulletins, please [login](#) or [join](#) our technical community.

DATE	ID
May 12, 2020	CA20-11
April 16, 2020	CA20-10
April 16, 2020	CA20-09
March 19, 2020	CA20-08
March 10, 2020	CA20-07
February 20, 2020	CA20-06
February 20, 2020	CA20-05
February 20, 2020	CA20-04
February 4, 2020	CA20-03
January 15, 2020	CA20-02

LOGIN OR JOIN OUR TECHNICAL COMMUNITY

詳細資訊請參考以下網址：<https://www.cyberark.com/product-security/>

特別備註：

在尚未進行 CyberArk 系統強化(Harden)前，請勿進行弱點掃描及進行任何的作業系統及漏洞更新，以避免 CyberArk 軟體在更新後無法正常運作。