Alibaba Cloud Threat Detection

安全警示

檔案版本：20190807

法律聲明

阿里雲提醒您在閱讀或使用本文檔之前仔細閱讀、充分理解本法律聲明各條款的內容。如果您閱讀或使用本文檔，您的閱讀或使用行為將被視為對本聲明全部內容的認可。

1. 您應當通過阿里雲網站或阿里雲提供的其他授權通道下載、擷取本文檔，且僅能用於自身的合法合規的商務活動。本文檔的內容視為阿里雲的保密資訊，您應當嚴格遵守保密義務；未經阿里雲事先書面同意，您不得向任何第三方披露本手冊內容或提供給任何第三方使用。
2. 未經阿里雲事先書面許可，任何單位、公司或個人不得擅自摘抄、翻譯、複製本文檔內容的部分或全部，不得以任何方式或途徑進行傳播和宣傳。
3. 由於產品版本升級、調整或其他原因，本文檔內容有可能變更。阿里雲保留在沒有任何通知或者提示下對本文檔的內容進行修改的權利，並在阿里雲授權通道中不時發布更新後的使用者文檔。您應當即時關注使用者文檔的版本變更並通過阿里雲授權渠道下載、擷取最新版的使用者文檔。
4. 本文檔僅作為使用者使用阿里雲產品及服務的參考性指引，阿里雲以產品及服務的”現狀“、“有缺陷”和“當前功能”的狀態提供本文檔。阿里雲在現有技術的基礎上盡最大努力提供相應的介紹及操作指引，但阿里雲在此明確聲明對本文檔內容的準確性、完整性、適用性、可靠性等不作任何明示或暗示的保證。任何單位、公司或個人因為下載、使用或信賴本文檔而發生任何差錯或經濟損失的，阿里雲不承擔任何法律責任。在任何情況下，阿里雲均不對任何間接性、後果性、懲戒性、偶然性、特殊性或刑罰性的損害，包括使用者使用或信賴本文檔而遭受的利潤損失，承擔責任（即使阿里雲已被告知該等損失的可能性）。
5. 阿里雲網站上所有內容，包括但不限於著作、產品、圖片、檔案、資訊、資料、網站架構、網站畫面的安排、網頁設計，均由阿里雲和/或其關係企業依法擁有其智慧財產權，包括但不限於商標權、專利權、著作權、商業秘密等。非經阿里雲和/或其關係企業書面同意，任何人不得擅自使用、修改、複製、公開傳播、改變、散布、發行或公開發表阿里雲網站、產品程式或內容。此外，未經阿里雲事先書面同意，任何人不得為了任何營銷、廣告、促銷或其他目的使用、公布或複製阿里雲的名稱（包括但不限於單獨為或以組合形式包含”阿里雲”、Aliyun”、“萬網”等阿里雲和/或其關係企業品牌，上述品牌的附屬標誌及圖案或任何類似公司名稱、商號、商標、產品或服務名稱、網域名稱、圖案標示、標誌、標識或通過特定描述使第三方能夠識別阿里雲和/或其關係企業）。
6. 如若發現本文檔存在任何錯誤，請與阿里雲取得直接聯絡。

通用約定

格式	說明	範例
	該類警示資訊將導致系統重大變更甚至故障，或者導致人身傷害等結果。	 **禁止:** 重設操作將丟失使用者配置資料。
	該類警示資訊可能導致系統重大變更甚至故障，或者導致人身傷害等結果。	 **警告:** 重啟操作將導致業務中斷，恢複業務所需時間約10分鐘。
	用於補充說明、最佳實務、竅門等，不是使用者必須瞭解的內容。	 **说明:** 您也可以通過按Ctrl + A選中全部檔案。
>	多級菜單遞進。	設定 > 網路 > 設定網路類型
粗體	表示按鍵、菜單、頁面名稱等UI元素。	單擊 確定。
`courier 字型`	命令。	執行 `cd / d C :/ windows` 命令，進入Windows系統檔案夾。
*## *	表示參數、變數。	`bae log list --instanceid` *Instance_ID*
[]或者[a|b]	表示可選項，至多選擇一個。	`ipconfig` *[-all|-t]*
{}或者{a|b}	表示必選項，至多選擇一個。	`swich` *{stand | slave}*

目錄

1 漏洞管理

1.1 漏洞修複必要性說明

保護雲上資產安全最重要的環節包括對漏洞修複進行優先順序評定。如果您擁有的資產數量較多，您可能在控制台看到數以千計的漏洞，這時優先修複哪些漏洞可能會成為您頭疼的難題。為瞭解決這個問題，Situation Awareness Service提供了一套新穎的評價標準，為您有序地修複漏洞提供參考。

漏洞修複建議得分

在評價一個Linux軟體漏洞或Windows系統漏洞是否應該優先修複時，Situation Awareness Service引入了漏洞修複建議得分，並根據漏洞修複建議得分將漏洞劃分為三個層級：需儘快修複、可延後修複、暫可不修複。

说明:

應急漏洞和WebCMS漏洞均為阿里雲安全工程師反覆確認後的高危漏洞，所以統一建議您儘快修複。

漏洞修複建議得分的計算方法如下：

漏洞修複建議得分 = 軟體漏洞的CVSS基礎分 * 時間因子 * 實際環境因子 * 資產重要性因子

其中，

- 軟體漏洞的CVSS基礎分：來源於該漏洞的CVSS2/3基礎分，取值範圍為0-10。
- 時間因子：彌補CVSS基礎分的不足，綜合了漏洞緩解措施被部署的時間延遲和漏洞利用方法的普及等因素後，形成的一條動態變化曲線，其取值範圍為0-1。

  在漏洞公開的前三天，由於曝光率的增加，該漏洞被利用的幾率會急劇增加，時間因子將從0增加並達到短暫的峰值（小於1），隨後急劇下降。隨著時間的推移，對漏洞成熟的利用手段將越來越多，漏洞實際利用難度在下降，時間因子將在100天之內逐漸增加並趨近於1。

- 實際環境因子：您的實際環境對判斷漏洞風險至關重要，我們對該漏洞利用所需的條件和您機器的情況進行綜合考慮，得出一個環境風險因數。

  當前納入參考的環境因素有：

  - 您的機器有對公網的流量：
    - 如果漏洞屬於一個可以遠程利用的漏洞，則環境因子為1.5。
    - 如果漏洞屬於一個可鄰網利用的漏洞，則環境因子為1.2。
    - 如果漏洞屬於本地利用，則環境因子為1。
    - 對某些需要雲上難以複現的環境來利用的漏洞，通過環境因子大幅降權。
  - 您的機器只有內網的流量：
    - 如果漏洞屬於一個可以遠程利用的漏洞，則通過環境因子大幅降權（設0）。
    - 如果漏洞屬於一個可鄰網利用的漏洞，則環境因子為1.2。
    - 如果漏洞屬於本地利用，則環境因子為1。
    - 對某些需要雲上難以複現的環境來利用的漏洞，通過環境因子大幅降權。
- 資產重要性因子：當機器數量很多時，系統為不同的機器/資產賦予不同使用情境下的重要性分值，並把該分值納入漏洞修複建議分的計算之中，為您有序修複漏洞提供有價值的參考。

  > 说明:
  > 資產重要性因子為預設 1。

從Situation Awareness Service發現漏洞到計算出漏洞的修複建議得分，大約有48小時的延遲。

> 说明:
> - 當一個漏洞剛被公布時，官方可能沒有給出其CVSS基礎分，這一部分漏洞的修複建議將會延遲到官方給出CVSS分後的48小時才能得出。
> - 由於您的Situation Awareness Service離線等網路異常問題可能導致環境因子無法計算，此時您需要等待網路環境恢複正常後的48小時才能看到修複建議。

漏洞修複建議（必要性）

- 需儘快修複：漏洞修複建議得分在13.5-15之間。
- 可延後修複：漏洞修複建議得分在7.1-13.5之間。
- 暫可不修複：漏洞修複建議得分在7以下。

特殊情況下的修複建議

- 當一個漏洞剛被掃描出來時，由於需要參照您的環境對參考分值進行加權，我們需要48小時的時間來評估修複建議。在這段時間內，漏洞的修複建議將依據漏洞本身的嚴重等級給出：
  - 如果該漏洞是嚴重漏洞：需儘快修複
  - 如果該漏洞是高危/中危漏洞：可延後修複
  - 如果該漏洞是低危漏洞：暫可不修複
- 由於網路抖動等原因我們無法擷取該漏洞的環境因子時，漏洞修複建議將統一為暫可不修複。

1.2 伺服器軟體漏洞修複

本文介紹了修複伺服器軟體漏洞的最佳實務方法。

當Situation Awareness Service的主機漏洞功能發現您伺服器上的漏洞後，您可參考以下方法來修複伺服器上的漏洞，保證漏洞修複工作的有效性和可靠性。

说明:

本方法適用於伺服器上的各類作業系統、網路裝置、資料庫、中介軟體的漏洞修複工作。

伺服器軟體漏洞修複方法

不同於普通PC上的漏洞修複，伺服器上的軟體漏洞修複應由具備一定專業知識的人員進行操作。漏洞修複工作的負責人應遵循以下修複流程：

修複前

1. 修複人員應對目標伺服器系統進行資產確認，並通過Situation Awareness Service對目標伺服器系統上的系統漏洞進行確認。關於Situation Awareness Service對Linux軟體漏洞的各項參數說明，請參考Linux軟體漏洞參數描述。
2. 修複人員在確認目標伺服器上的系統漏洞後，應確認哪些系統漏洞需要修複。並不是所有被發現的軟體漏洞都需要在第一時間進行修複，應根據實際業務情況、伺服器的使用方式、及漏洞修複可能造成的影響來判定漏洞是否需要修複。
3. 修複人員在測試環境中部署待修複漏洞的相關補丁，從相容性和安全性方面進行測試，並在測試完成後形成漏洞修複測試報告。漏洞修複測試報告應包含漏洞修複情況、漏洞修複的時間長度、補丁本身的相容性、及漏洞修複可能造成的影響。
4. 為了防止出現不可預料的後果，在正式開始漏洞修複前，修複人員應使用備份恢複系統對待修複的商務服務器系統進行備份。例如，通過ECS的快照功能備份目標ECS執行個體。

修複中

1. 在目標伺服器部署修複漏洞的相關補丁及進行修複操作時，應至少有兩名修複人員在場（一人負責操作，一人負責記錄），盡量防止可能出現的誤操作。
2. 修複人員按照待修複的系統漏洞列表，逐項進行升級、修複。

修複後

1. 修複人員對目標伺服器系統上的漏洞修複進行驗證，確保漏洞已修複且目標伺服器沒有出現任何異常情況。
2. 修複人員對整個漏洞修複過程進行記錄，形成最終漏洞修複報告，並將相關文檔進行歸檔。

伺服器軟體漏洞補丁修複風險規避措施

為了確保在伺服器軟體漏洞修複過程中目標伺服器系統的正常運行、並將異常情況發生的可能性降到最低，在漏洞修複過程中應採取以下風險規避措施：

- 制定漏洞修複方案

  漏洞修複負責人應對修複對象（目標伺服器）啟動並執行作業系統和應用系統進行調研，並制定合理的漏洞修複方案。漏洞修複方案應通過可行性論證，並得到實際環境的測實驗證支援。漏洞修複實施工作應嚴格按照漏洞修複方案所確定的內容和步驟進行，確保每一個操作步驟都對目標商務服務器系統沒有損害。

- 使用模擬測試環境

  通過使用模擬測試環境，對漏洞補丁修複方案進行驗證，證明制定的漏洞補丁修複方案對待修複的線上業務系統沒有損害。

  > 说明:
  > 模擬測試環境要求系統內容（作業系統、資料庫系統）與線上業務系統完全一致，應用系統也與線上業務系統的版本一致，資料建議採用線上業務系統最近一次的全備份資料。

- 進行系統備份

  對整個業務系統進行完全備份，包括系統、應用軟體和資料。備份完成後，應對系統備份的資料進行有效性恢複驗證。通過系統備份，當發生系統內容異常或資料丟失時，可以及時對系統進行恢複，確保業務穩定。建議使用ECS的快照功能對業務系統進行快速、高效的備份。

2 基準配置核查

2.1 主機基準核查

Situation Awareness Service支援和雲產品基準檢測服務雲產品上存配置項，並提供修複建議。本文介紹了使用主機基準核查檢測並修複伺服器上不安全配置的操作方法。

功能描述

主機基準核查功能在啟用後，自動偵測伺服器上的系統、帳號、資料庫、弱密碼、合格性配置中存在的風險點，並提供修複建議。具體檢測內容，參見文末主機基準核查檢測內容。

主機基準核查的預設策略為每天進行一次全面自動檢測，在6-12點間完成。您可以自行添加和維護檢測原則範本，自訂需要檢查的項目、生效的伺服器、檢查周期、和觸發時間。

说明:

某些檢測項（例如，MySQL弱密碼檢測、SQLServer弱密碼檢測）可能採用嘗試登入的方式進行檢測，從而會佔用一定的伺服器資源，生產較多的登入失敗記錄。這些檢查項目預設是關閉。如果您需要這些功能，請確認上述風險後，在自訂主機基準核查原則範本時勾選這些檢測項目。

主機基準核查也支援白名單設定，允許您徹底忽略某些主機基準核查項目，Situation Awareness Service不會檢測主機基準核查白名單中的項目。加入白名單或忽略操作支援填寫備忘（如忽略的原因），以便後續回溯分析。

添加主機基準核查原則範本

開通主機基準核查後，Situation Awareness Service將使用預設原則範本（在每天6-12點）對指定資產進行檢測。預設原則範本的檢測項不可更改，但您可以調整預設原則範本的生效伺服器。

如果您需要自訂掃描策略和檢測項目，您可以參照以下步驟，建立一個掃描原則範本：

1. 登入雲盾Situation Awareness Service控制台。
2. 在左側導覽列，單擊基準配置核查。

3. 單擊添加原則範本，建立一個掃描原則範本，完成以下配置：

   a. 輸入用於識別該模板的名稱。

   b. 勾選需要檢測的項目，在合規性檢測、弱密碼檢測、系統、帳號、資料庫下勾選具體檢測內容，詳情參見文末主機基準核查檢測內容。

   c. 選擇檢測周期（每1天/3天/7天/30天檢測一次）和檢測觸發時間（0-6點、6-12點、12-18點、18-24點）。

   d. 勾選應用上述設定的分組資產。

   > 说明:
   > 新建立的伺服器預設歸屬在分組資產 > 未分組，如需對新建立資產自動應用該模板，請勾選未分組。

   e. 單擊提交，完成建立。

   已添加原則範本自動生效，按照配置的周期和觸發時間自動執行掃描任務。您也可以在主機基準分頁下，單擊原則範本下的立即檢測，立即執行該掃描任務。

4. 對於已添加的模板，您可以單擊基準配置核查頁面右上方的基準檢查設定；然後在掃描策略下，選擇相應模板，單擊編輯修改其內容，或單擊刪除移除該模板。

查看和修複風險配置

參照以下步驟，查看並修複您伺服器上的風險配置項：

1. 登入雲盾Situation Awareness Service控制台。
2. 在左側導覽列，單擊基準配置核查。
3. 在主機基準分頁下，查看您伺服器上存在的配置風險項。
4. 使用風險搜尋和頁簽篩選功能，快速定位到具體風險。

   > 说明:
   > 只有選擇一個具體的風險分類後，才可以進一步選擇對應的風險子分類。

5. 在主機基準分頁，根據需要執行以下操作：

   - 勾選風險項，單擊風險列表下方的忽略，忽略該風險警示；忽略風險後，該風險不再觸發警示。
   - 勾選風險項，單擊風險列表下方的加入白名單，將風險項加入白名單；將風險項加入白名單後，Situation Awareness Service將不去檢測該風險。

6. 選擇一個風險項，單擊其名稱，進入風險詳情頁面，查看該風險的詳細資料和受影響的資產。

7. 參照風險詳情 > 更多 下的加固或修複建議，在對應伺服器上進行修複。

> 说明:
> 您可以勾選一個或多個受影響資產，使用影響資產列表下方的批量操作按鈕執行批量操作。

- 修複風險後，單擊操作列中的驗證，一鍵驗證該風險是否已修複成功。如果您未進行手動驗證，風險修複成功後 72 小時內Situation Awareness Service會自動驗證。
- 如果您不希望收到該風險項的警示，您可以單擊操作列中的忽略，忽略該風險，已忽略風險不會觸發警示。
- 如果您希望徹底忽略該風險項，不再對其進行檢測，您可以單擊頁面右上方的加入白名單，並添加備忘資訊。添加進白名單中的風險項可在主機基準核查設定中恢複。

主機基準核查設定

參照以下步驟，使用主機基準核查的設定功能：

1. 登入雲盾Situation Awareness Service控制台。
2. 在左側導覽列，單擊基準配置核查。
3. 單擊頁面右上方的基準檢測設定。您可以執行以下設定：

- 編輯或刪除掃描原則範本。具體見添加主機基準核查原則範本。
- 選擇失效風險自動刪除周期：7天、30天、90天。

> 说明:
> 對檢測出來的風險項不做任何處理的話，該風險項預設失效，並在指定的周期後被自動刪除。

- 維護基準白名單：單擊一個風險項下的移除，將其從白名單中移除，系統將重新對其進行檢測和警示。

主機基準核查檢測內容

分類	檢測項
合規基準檢測	Httpd2.2中介軟體合規基準檢測
	Windows 2008 R2系統合規基準檢測
	Memcached基準檢測
	Centos7系統基準合規檢測
	MySQL5.6資料庫合規基準檢測
	SQLServer_2008_r2合規基準檢測
	Tomcat7中介軟體基準合規檢測

	MongoDB基準檢測
	Ubuntu14系統合規基準檢測
弱密碼檢測	Postgre弱密碼檢測
	SSH弱密碼檢測
	FTP匿名登入檢測
	SQLServer弱密碼檢測
	MySQL弱密碼檢測
	RDP弱密碼檢測
	FTP弱密碼檢測
系統	組策略
	基準策略
	系統檔案變動監控
	註冊表
帳號	系統賬戶安全
資料庫	Redis合規檢查