阿里云
云安全中心（态势感知）

安全防范

文档版本：20190919

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。
2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。
3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。
4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的”现状“、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。
5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含”阿里云”、Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。
6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **禁止:** 重置操作将丢失用户配置数据。
	该类警示信息可能导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **警告:** 重启操作将导致业务中断，恢复业务所需时间约10分钟。
	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 **说明:** 您也可以通过按Ctrl + A选中全部文件。
>	多级菜单递进。	设置 > 网络 > 设置网络类型
粗体	表示按键、菜单、页面名称等UI元素。	单击 **确定**。
`courier` 字体	命令。	执行 `cd /d C:/windows` 命令，进入Windows系统文件夹。
*## *	表示参数、变量。	`bae log list --instanceid` *`Instance_ID`*
[]或者[a|b]	表示可选项，至多选择一个。	`ipconfig` *`[-all|-t]`*
{}或者{a|b}	表示必选项，至多选择一个。	`swich` *`{stand | slave}`*

目录

1 漏洞修复

1.1 漏洞修复必要性说明

阿里云云安全中心可提供Linux软件漏洞、Windows系统漏洞、Web-CMS漏洞、应用漏洞和应急漏洞的检测和修复服务。

保护云上资产安全最重要的环节包括对漏洞修复进行优先级评定。如果您拥有的资产数量较多，您可能在控制台看到多个漏洞，这时优先修复哪些漏洞可能会成为您头疼的难题。为了解决这个问题，云安全中心提供了一套新颖的评价标准，为您有序地修复漏洞提供参考。

漏洞修复建议得分

在评价一个Linux软件漏洞、应用漏洞或Windows系统漏洞是否应该优先修复时，云安全中心引入了漏洞修复建议得分，并根据漏洞修复建议得分将漏洞划分为三个级别：需尽快修复、可延后修复、暂可不修复。

说明:

应急漏洞和WebCMS漏洞均为阿里云安全工程师反复确认后的高危漏洞，所以统一建议您尽快修复。

漏洞修复建议得分的计算方法如下：

漏洞修复建议得分 = 软件漏洞的CVSS基础分 * 时间因子 * 实际环境因子 * 资产重要性因子

其中参数解释如下：

- 软件漏洞的CVSS基础分：来源于该漏洞的CVSS2/3基础分，取值范围为0-10。
- 时间因子：弥补CVSS基础分的不足，综合了漏洞缓解措施被部署的时间延迟和漏洞利用方法的普及等因素后，形成的一条动态变化曲线，其取值范围为0-1。

  在漏洞公开的前三天，由于曝光率的增加，该漏洞被利用的几率会急剧增加，时间因子将从0增加并达到短暂的峰值（小于1），随后急剧下降。随着时间的推移，对漏洞成熟的利用手段将越来越多，漏洞实际利用难度在下降，时间因子将在100天之内逐渐增加并趋近于1。

- 实际环境因子：您的实际环境对判断漏洞风险至关重要，我们对该漏洞利用所需的条件和您机器的情况进行综合考虑，得出一个环境风险因数。

  当前纳入参考的环境因素有：

  - 您的机器有对公网的流量：
    - 如果漏洞属于一个可以远程利用的漏洞，则环境因子为1.5。
    - 如果漏洞属于一个可邻网利用的漏洞，则环境因子为1.2。
    - 如果漏洞属于本地利用，则环境因子为1。
    - 对某些需要云上难以复现的环境来利用的漏洞，通过环境因子大幅降权。
  - 您的机器只有内网的流量：
    - 如果漏洞属于一个可以远程利用的漏洞，则通过环境因子大幅降权（设0）。
    - 如果漏洞属于一个可邻网利用的漏洞，则环境因子为1.2。
    - 如果漏洞属于本地利用，则环境因子为1。
    - 对某些需要云上难以复现的环境来利用的漏洞，通过环境因子大幅降权。
- 资产重要性因子：当机器数量很多时，系统为不同的机器/资产赋予不同使用场景下的重要性分值，并把该分值纳入漏洞修复建议分的计算之中，为您有序修复漏洞提供有价值的参考。

  > 说明:
  > 资产重要性因子为默认 1。

从云安全中心发现漏洞到计算出漏洞的修复建议得分，大约有48小时的延迟。

> 说明:
> - 当一个漏洞刚被公布时，官方可能没有给出其CVSS基础分，这一部分漏洞的修复建议将会延迟到官方给出CVSS分后的48小时才能得出。
> - 由于您的云安全中心离线等网络异常问题可能导致环境因子无法计算，此时您需要等待网络环境恢复正常后的48小时才能看到修复建议。

漏洞修复建议（必要性）

- 需尽快修复：漏洞修复建议得分在13.5-15之间。
- 可延后修复：漏洞修复建议得分在7.1-13.5之间。
- 暂可不修复：漏洞修复建议得分在7以下。

特殊情况下的修复建议

- 当一个漏洞刚被扫描出来时，由于需要参照您的环境对参考分值进行加权，我们需要48小时的时间来评估修复建议。在这段时间内，漏洞的修复建议将依据漏洞本身的严重等级给出：
  - 如果该漏洞是严重漏洞：需尽快修复
  - 如果该漏洞是高危/中危漏洞：可延后修复
  - 如果该漏洞是低危漏洞：暂可不修复
- 由于网络抖动等原因我们无法获取该漏洞的环境因子时，漏洞修复建议将统一为暂可不修复。

1.2 Linux软件漏洞

本文档介绍了云安全中心检测到的Linux软件漏洞详细信息以及相关操作。

背景信息

云安全中心基础版只提供漏洞检测，不提供漏洞修复的服务；如需一键修复漏洞，请开通云安全中心高级版或企业版。基础版、高级版和企业版详细功能介绍参见#unique_6。

查看漏洞基本信息

1. 登录云安全中心控制台。
2. 在左侧导航栏，单击安全防范 > 漏洞修复，打开漏洞修复页面，单击Linux软件漏洞。

3. 您可在Linux软件漏洞页面的漏洞列表中，查看云安全中心检测到的Linux漏洞关联的漏洞公告，漏洞公告名称通常以*USN*、*RHSA*或*CVE*字符开头。

   · 查看漏洞公告信息

   · 查看漏洞的修复紧急度建议

   漏洞的建议修复紧急度用不同颜色的图标表示，图标中的数字表示对应紧急度的待处理漏洞个数。

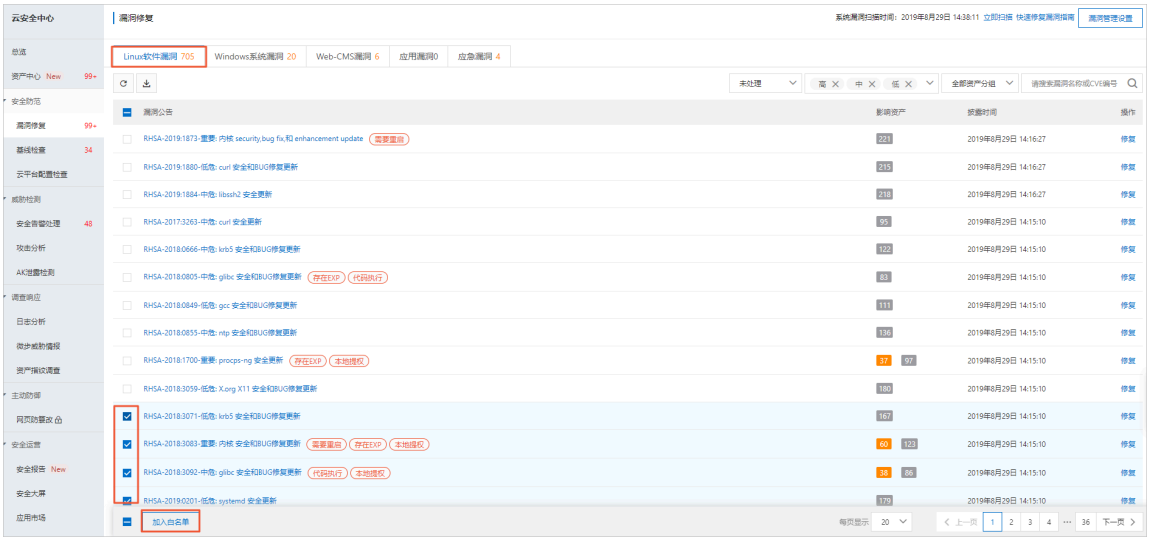
   - 红色图标表示云安全中心判定该漏洞修复紧急程度高
   - 橙色图标表示云安全中心判定该漏洞修复紧急程度中
   - 灰色图标表示云安全中心判定该漏洞修复紧急程度低

说明:

建议立即修复高危漏洞（紧急程度高）。

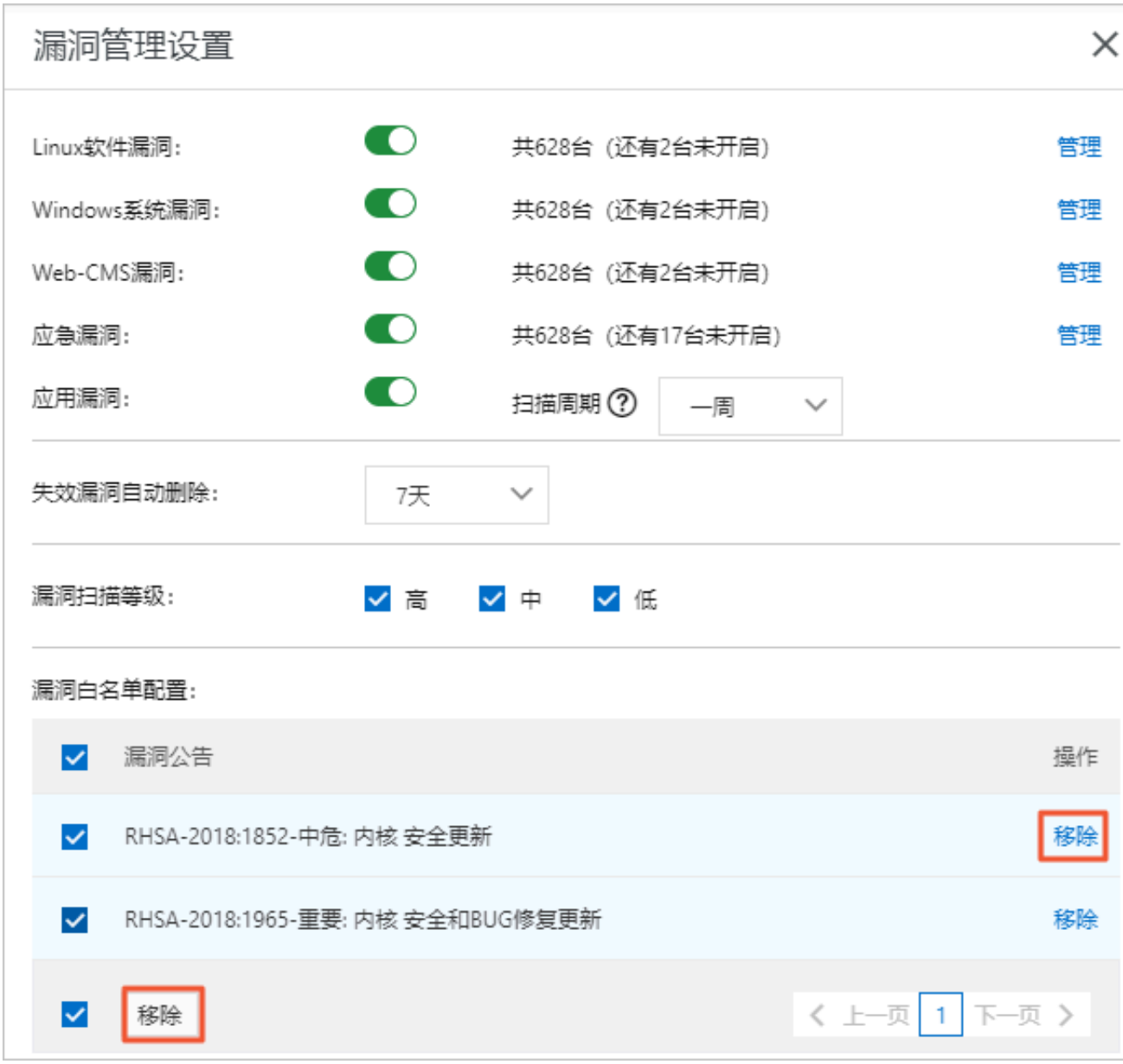
- **将漏洞加入白名单**

  您可在Linux软件漏洞页面，勾选漏洞列表左侧的复选框后，单击加入白名单，将该漏洞加入白名单中。加入白名单后，云安全中心将不再对白名单中的漏洞进行告警。



加入白名单的漏洞将从Linux软件漏洞的漏洞列表中移除，并记录在漏洞管理设置页面的漏洞白名单配置列表中。

如需恢复云安全中心对白名单中的漏洞进行检测和告警提示，可在漏洞管理设置页面移除该漏洞。



- **搜索漏洞**

  您可在Linux软件漏洞页面，通过筛选漏洞危险等级（高、中、低）、漏洞处理状态（已处理、未处理）、资产分组或输入漏洞名称定位到相关的漏洞。

说明:

搜索漏洞名称支持模糊查询。

- 导出漏洞

  您可在Linux软件漏洞页面单击导出按钮，将云安全中心检测到的所有Linux系统漏洞统一导出并保存到本地。导出的文件为Excel格式。

  说明:

  根据您资产中漏洞数据的大小，导出漏洞列表可能需要耗费一定时间，请耐心等待。

查看漏洞详情和处理漏洞

1. 登录云安全中心控制台。
2. 在左侧导航栏，单击安全防范 > 漏洞修复，打开漏洞修复页面，单击Linux软件漏洞。
3. 在漏洞列表，单击漏洞公告名称或漏洞公告对应操作栏下的修复，可展开对应的漏洞详情页面。

   您可查看该漏洞公告的漏洞详情和待处理漏洞数量及待处理漏洞关联资产。

4. 在漏洞详情页面，您可根据需要执行以下步骤查看漏洞详情，并处理漏洞。

· 查看漏洞详情

漏洞详情页面可展示该漏洞公告所有关联漏洞，及漏洞影响的所有资产信息，方便您对所有相关的漏洞进行分析和批量处理。

- 单击漏洞详情页签，您可在漏洞详情子页查看该漏洞公告关联的所有漏洞、漏洞的描述、漏洞紧急程度。
- 单击待处理漏洞页签，直接跳至漏洞详情下的漏洞影响资产列表。

  您可在漏洞影响资产列表，查看该漏洞影响的所有资产、漏洞的状态等信息，并可对漏洞执行验证、修复、加入白名单、忽略或回滚的操作。

在漏洞详情页面的漏洞列表中，单击影响资产下的资产名称，可定位到资产中心 > 漏洞信息页面，为您展示该资产所有关联漏洞的信息。

· 查看阿里云漏洞库详细信息

在Linux漏洞详情页面，单击漏洞编号可跳转至阿里云漏洞库。

您可在 阿里云漏洞库 页面，查看该漏洞更加详细的信息，包括漏洞的详细描述、危险等级、披露时间、修复建议等信息。

· 查看漏洞严重等级

漏洞紧急程度用不同颜色的图标表示：红色图标表示高危漏洞、橙色图标表示中危漏洞、灰色图标表示低危漏洞。

说明:

建议立即修复高危漏洞（紧急程度高）。

- 查看漏洞修复的关联进程

  您可在漏洞详情页面，单击关联进程栏的图标，查看漏洞关联进程，帮助您了解修复该漏洞可能会影响的进程或业务系统。

- 查看漏洞详细状态
  - 已处理
    - 修复成功：漏洞已执行一键修复并修复成功。
    - 修复失败：漏洞修复失败，可能因为漏洞文件已被修改或漏洞文件已不存在。
    - 已忽略：漏洞已执行忽略的操作，云安全中心将不再对该漏洞进行告警。
    - 漏洞已失效：表示该漏洞在7天内未被再次扫描到。
    - 回滚失败：漏洞回滚失败、无法回到未处理状态，可能因为漏洞文件已不存在。

     说明:

已处理的漏洞支持回滚操作，漏洞回滚后将重新变为未处理的状态。

- 未处理：未修复，即漏洞待修复。

· 处理受影响资产漏洞

您可对受影响资产漏洞进行修复、验证、加白名单、忽略或回滚的操作。

- 修复漏洞

  您可在漏洞详情页面单击修复，单个修复漏洞进行或批量修复多个关联漏洞。

- 验证漏洞

  您可在漏洞详情页面，验证单个漏洞或批量验证多个关联漏洞，检测该漏洞是否已修复成功。

  单击验证后，该漏洞的状态转为验证中。需要等待数秒后漏洞验证才可完成。

- 将漏洞加入白名单

  您可在漏洞详情页面，单击右上角加入白名单，将该漏洞加入白名单中。加入白名单后，云安全中心将不再对白名单中的漏洞进行告警。

  加入白名单的漏洞将从Linux软件漏洞的漏洞列表中移除，并记录在漏洞管理设置页面的漏洞白名单配置列表中。

  如需恢复云安全中心对白名单中的漏洞进行检测和告警提示，可在漏洞管理设置页面移除该漏洞。

- 忽略漏洞

  您可在漏洞详情页面，勾选漏洞列表左侧的复选框后，单击并选择忽略，云安全中心将不再提示该漏洞。

说明：

被忽略的漏洞状态将转为已忽略。如需云安全中心继续对该漏洞进行告警提示，可在已处理的漏洞列表中找到该漏洞并对其取消忽略。

- 回滚漏洞

  您可在漏洞详情页面，勾选漏洞列表左侧的复选框后单击并选择回滚，选择待回滚快照，单击确认。

- 搜索漏洞影响资产

  您可在漏洞详情页面，通过筛选漏洞危险等级（高、中、低）、资产分组、漏洞处理状态（已处理、未处理）或输入服务器IP或名称定位到相关的漏洞影响的资产。

  说明:
  搜索服务器IP或名称支持模糊查询。

- 导出漏洞影响资产

  您可在漏洞详情页面，单击导出按钮 ，将云安全中心检测到的该Linux系统漏洞下影响资产统一导出并保存到本地。导出的文件为Excel格式。

  说明:
  根据您资产中漏洞数据的大小，导出漏洞列表可能需要耗费一定时间，请耐心等待。

- 保存已筛选漏洞

  您可在漏洞详情页面，单击 按钮保存筛选出的所有漏洞为一个漏洞修复批次，方便您对该批次漏洞的状态进行持续跟踪。

Linux软件漏洞详情页说明

漏洞详情页项目	描述
漏洞编号	该漏洞对应的CVE漏洞号。Common Vulnerabilities & Exposures（CVE）是已被广泛认同的信息安全漏洞或者已经暴露的弱点的公共名称。通过漏洞编号（如*CVE-2018-1123*），您可以快速地在任何其它CVE兼容的数据库中找到相应漏洞修复的信息，帮助您解决安全问题。

漏洞详情页项目	描述
影响分（CVSS分值）	CVSS分值遵循被广泛采纳的行业标准 - 通用漏洞评分系统（Common Vulnerability Scoring System），根据漏洞的多种属性通过公式计算得出。主要用于量化漏洞的严重程度。 在CVSS v3.0评分体系中，不同分值代表的漏洞严重程度如下： · 0.0：无漏洞 · 0.1-3.9：低危 - 可导致本地拒绝服务的漏洞。 - 其他危害较低的漏洞。 · 4.0-6.9：中危 - 需要进行交互才能影响用户的漏洞。 - 可导致普通越权操作的漏洞。 - 通过本地修改配置或获取信息之后，可进一步利用的漏洞。 · 7.0-8.9：高危 - 可间接获取服务器和应用系统的普通权限的漏洞。 - 可导致任意文件读取、下载、写入、或删除的漏洞。 - 可导致敏感信息泄漏的漏洞。 - 可直接导致业务中断、或远程拒绝服务的漏洞。 · 9.0-10.0：严重 - 可直接获取服务器系统权限的漏洞。 - 可直接获取重要的敏感信息，导致数据泄漏的漏洞。 - 可直接导致敏感信息越权访问的漏洞。 - 可造成大范围影响的其他漏洞。
影响资产	存在该漏洞的服务器资产信息，包括资产的公网/私网IP地址等。

漏洞详情页项目	描述
紧急程度	漏洞的严重等级，包括： · 紧急程度高： 高风险漏洞，建议尽快修复。 · 紧急程度中： 中危漏洞，您可根据业务需要尽快修复或延后修复。 · 紧急程度低： 低风险漏洞，您可根据业务需要尽快修复或暂不修复。 您可参考#unique_8。
详情	您可单击漏洞详情页面右侧详情查看修复命令、漏洞命中原因等信息。 · 修复命令：执行该命令可修复对应的Linux软件漏洞。 · 影响说明： - 软件：该软件在当前服务器系统中的版本信息。 - 命中：该漏洞的匹配命中原因，一般是由于当前软件版本不满足或者小于某个版本（以小于某个版本为主）。 - 路径：该软件在服务器上的路径。 · 风险重要提醒：关于漏洞的风险提醒、补充修复建议和参考文档。

1.3 Windows系统漏洞

云安全中心支持Windows系统漏洞检测和修复的功能。

背景信息

通过实时同步微软官网补丁源，对高危及有影响的漏洞进行有效的检测和告警，避免攻击者通过Windows系统漏洞对您的服务器进行攻击或威胁您服务器的数据安全。

> 说明:
> 云安全中心基础版只提供漏洞检测，不提供漏洞修复的服务；如需一键修复漏洞，请开通云安全中心高级版或企业版。基础版、高级版和企业版详细功能介绍参见#unique_6。

查看漏洞基本信息

1. 登录云安全中心控制台。
2. 在左侧导航栏，单击安全防范 > 漏洞修复，打开漏洞修复页面，单击Windows系统漏洞。

3. 在Windows系统漏洞页面，查看和管理云安全中心检测到的所有Windows系统漏洞信息。

- 查看漏洞信息

- 查看漏洞的修复紧急度建议

漏洞的建议修复紧急度用不同颜色的图标表示，图标中的数字表示对应紧急度的待处理漏洞个数。

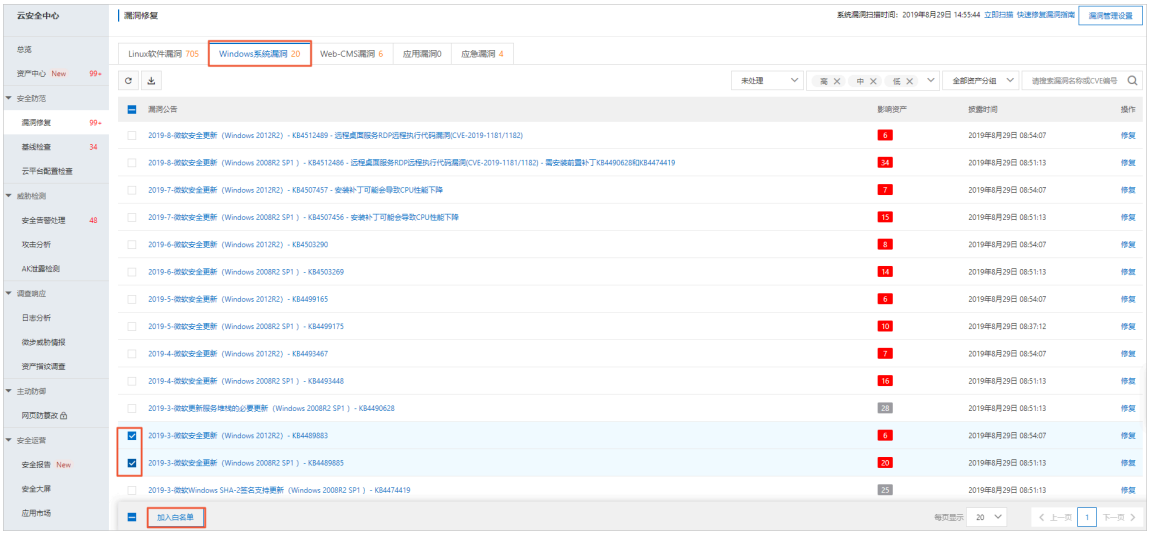
- 红色图标表示云安全中心判定该漏洞修复紧急程度高
- 橙色图标表示云安全中心判定该漏洞修复紧急程度中
- 灰色图标表示云安全中心判定该漏洞修复紧急程度低

说明:

建议立即修复高危漏洞（紧急程度高）。

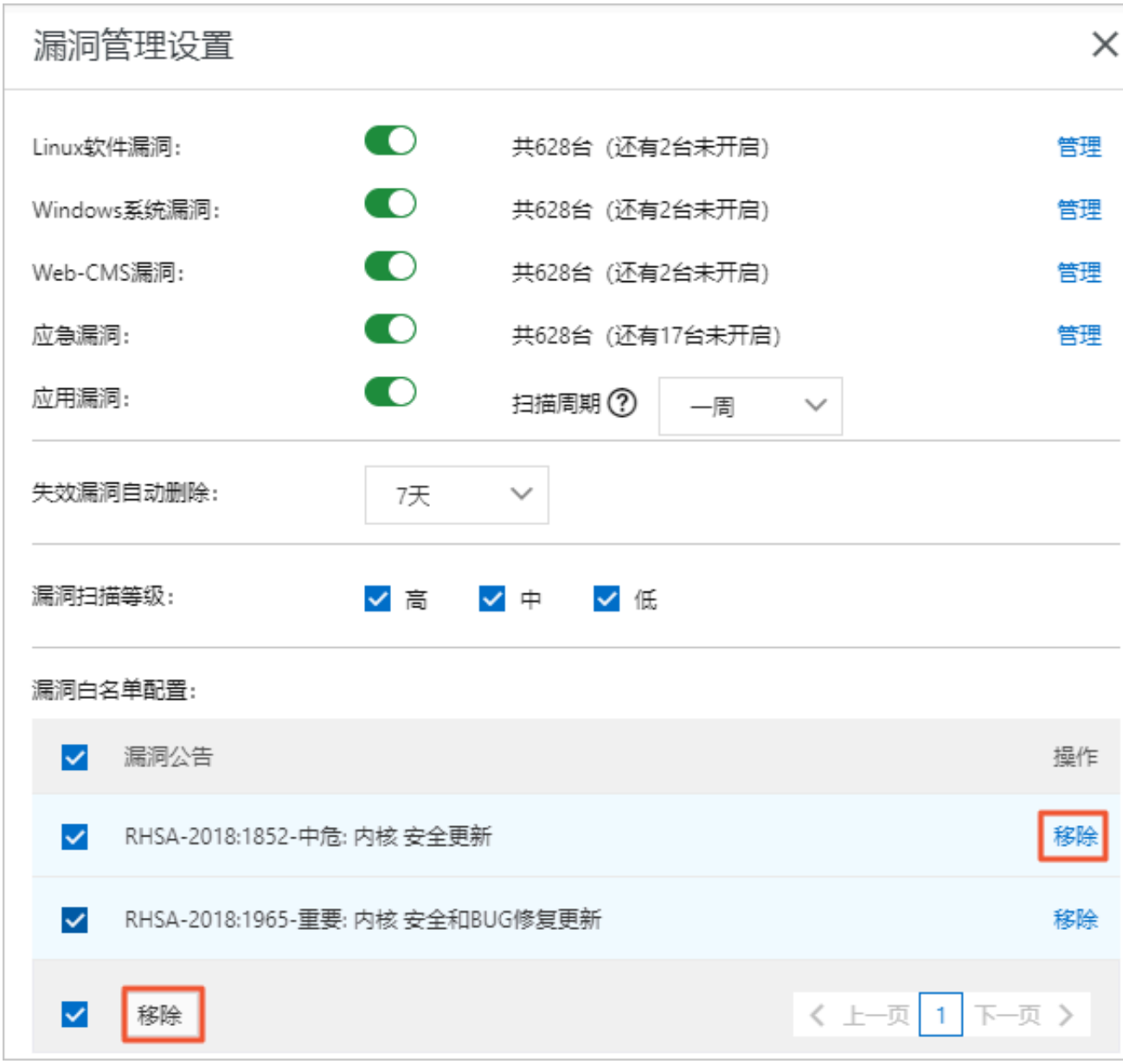
- **将漏洞加入白名单**

  您可在Windows系统漏洞页面，勾选漏洞列表左侧的复选框后单击加入白名单，将该漏洞加入白名单中。加入白名单后，云安全中心将不再对白名单中的漏洞进行告警。



加入白名单的漏洞将从Windows系统漏洞的漏洞列表中移除，并记录在漏洞管理设置页面的漏洞白名单配置列表中。

如需恢复云安全中心对白名单中的漏洞进行检测和告警提示，可在漏洞管理设置页面移除该漏洞。



- **搜索漏洞**

  您可在Windows系统漏洞页面通过筛选漏洞危险等级（高、中、低）、漏洞处理状态（已处理、未处理）、资产分组或输入漏洞名称定位到相关的漏洞。

说明:

搜索漏洞名称支持模糊查询。

- 导出漏洞

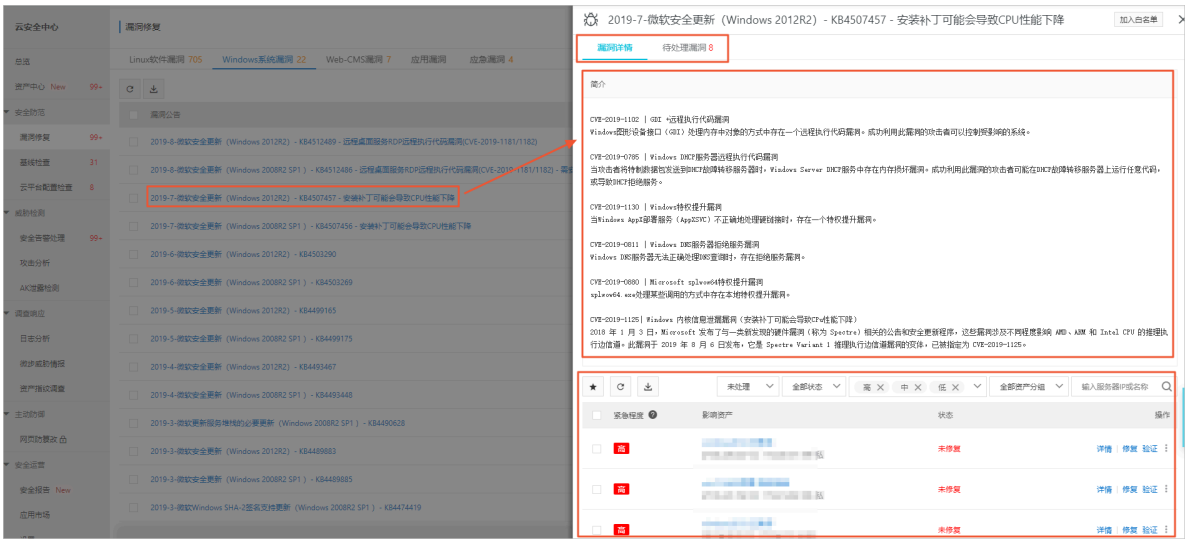
  您可在Windows系统漏洞页面，单击导出按钮，将云安全中心检测到的所有Linux系统漏洞统一导出并保存到本地。导出的文件为Excel格式。

  说明:
  根据您资产中漏洞数据的大小，导出漏洞列表可能需要耗费一定时间，请耐心等待。

查看漏洞详情和处理漏洞

1. 登录云安全中心控制台。
2. 在左侧导航栏，单击安全防范 > 漏洞修复，打开漏洞修复页面，单击Windows系统漏洞。
3. 在漏洞列表，单击漏洞公告名称或漏洞公告对应操作栏下的修复，可展开对应的漏洞详情页面。

   您可查看该漏洞的漏洞详情简介和待处理漏洞数量及待处理漏洞关联资产。



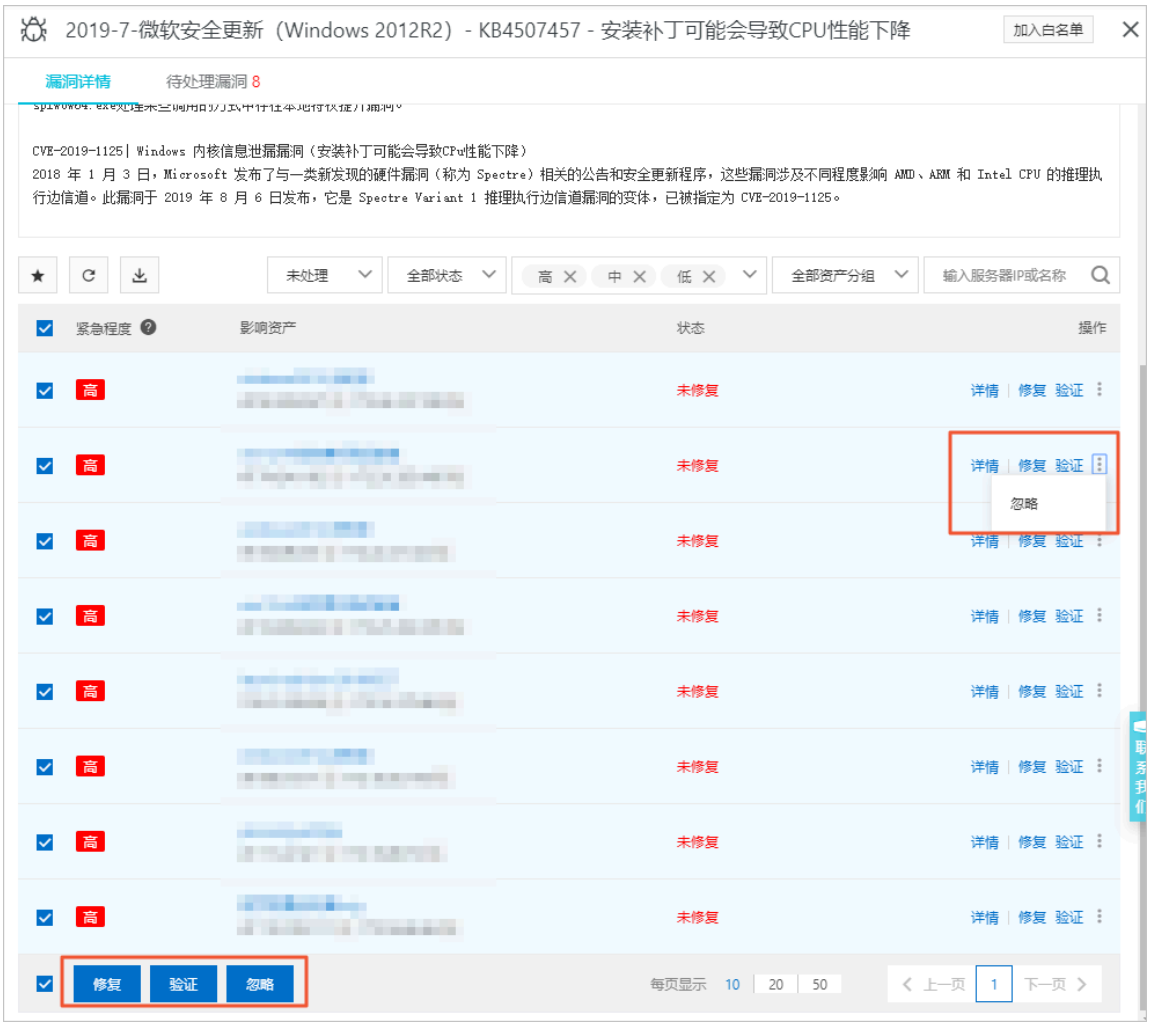
4. 在漏洞详情页面，您可以根据需要执行以下步骤查看漏洞详情，并处理漏洞。

- 查看漏洞详情

  漏洞详情页面可展示该漏洞所有关联漏洞，即该漏洞影响的所有资产信息，方便您对所有相关的漏洞进行分析和批量处理。

  - 单击漏洞详情页签，您可在漏洞详情子页查看该漏洞公告关联的所有漏洞简介。
  - 单击待处理漏洞页签，直接跳至漏洞详情下的漏洞影响资产列表。

    您可在漏洞影响资产列表，查看该漏洞影响的所有资产、漏洞的状态等信息，并可对漏洞执行验证、修复、加入白名单、忽略或回滚的操作。



- 查看漏洞严重等级

  漏洞紧急程度用不同颜色的图标表示：红色图标表示高危漏洞、橙色图标表示中危漏洞、灰色图标表示低危漏洞。

说明:

建议立即修复高危漏洞（紧急程度高）。

- 查看漏洞详细状态
  - 已处理
    - 修复成功：漏洞已执行一键修复并修复成功。
    - 修复失败：漏洞修复失败，可能因为漏洞文件已被修改或漏洞文件已不存在。
    - 已忽略：漏洞已执行忽略的操作，云安全中心将不再对该漏洞进行告警。
    - 漏洞已失效：表示该漏洞在7天内未被再次扫描到。
    - 回滚失败：漏洞回滚失败、无法回到未处理状态，可能因为漏洞文件已不存在。

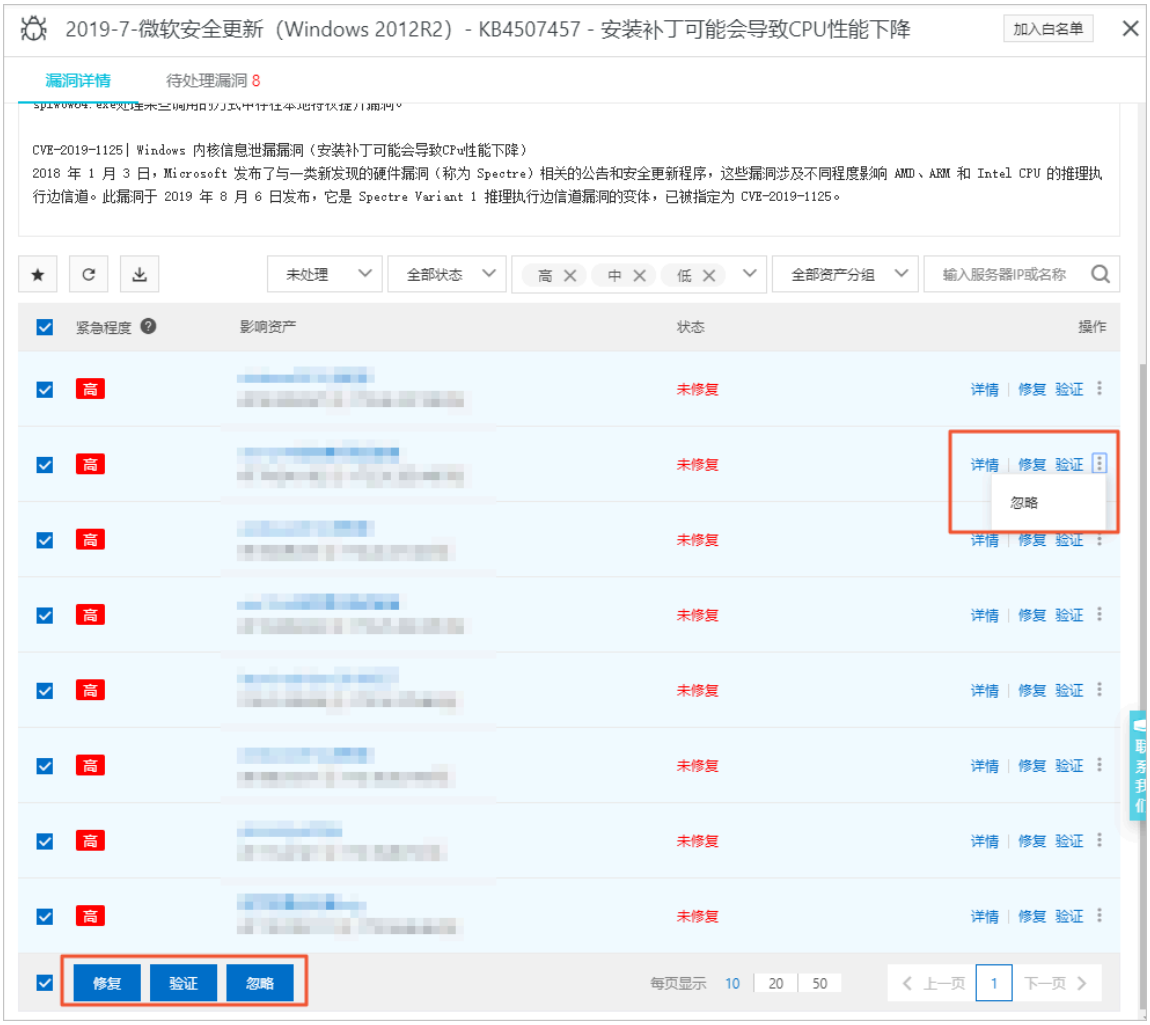
 说明：

已处理的漏洞支持回滚操作，漏洞回滚后将重新变为未处理的状态。

- 未处理：未修复，即漏洞待修复。

· 处理受影响资产漏洞

您可对受影响资产漏洞进行修复、验证、加白名单、忽略或回滚的操作。



- 修复漏洞

  您可在漏洞详情页面，单击修复，单个修复漏洞或批量修复多个关联漏洞。

- 验证漏洞

  您可在漏洞详情页面，验证单个漏洞或批量验证多个关联漏洞，检测该漏洞是否已修复成功。

  单击验证后，该漏洞的状态转为验证中。需要等待数秒后漏洞验证才可完成。

- 将漏洞加入白名单

  您可在漏洞详情页面，单击右上角加入白名单，将该漏洞加入白名单中。加入白名单后，云安全中心将不再对白名单中的漏洞进行告警。

加入白名单的漏洞将从Windows系统漏洞的漏洞列表中移除，并记录在漏洞管理设置页面的漏洞白名单配置列表中。

如需恢复云安全中心对白名单中的漏洞进行检测和告警提示，可在漏洞管理设置页面移除该漏洞。

- 忽略漏洞

  您可在漏洞详情页面，勾选漏洞列表左侧的复选框后，单击并选择忽略，云安全中心将不再提示该漏洞。

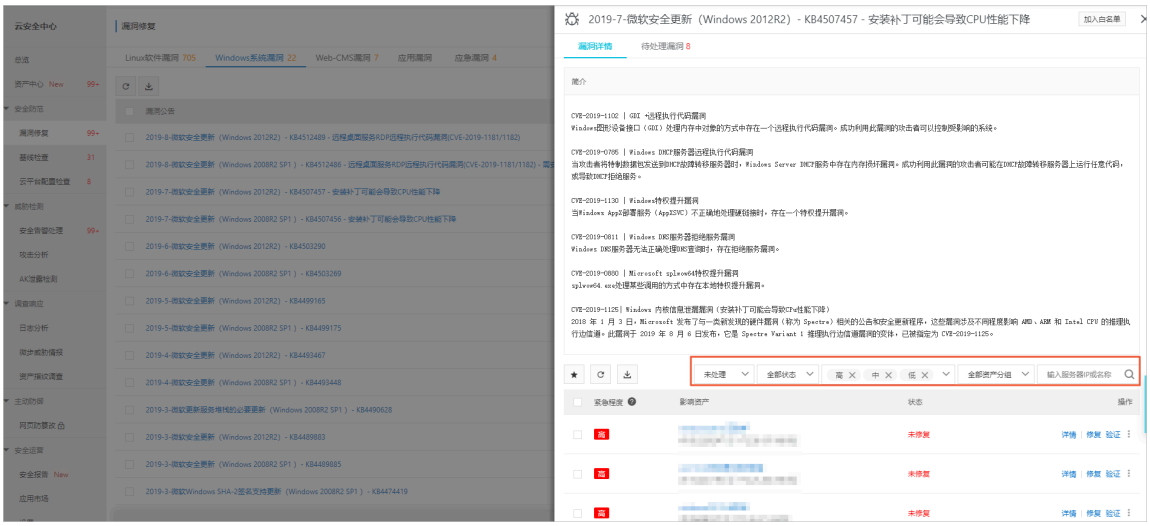
  > **说明:**
  > 被忽略的漏洞状态将转为已忽略。如需云安全中心继续对该漏洞进行告警提示，可在已处理的漏洞列表中找到该漏洞并对其取消忽略。

- 回滚漏洞

  云安全中心支持对已处理的漏洞，进行回滚操作，漏洞回滚后将重新变为未处理的状态。

· 搜索漏洞影响资产

您可在漏洞详情页面，通过筛选漏洞危险等级（高、中、低）、资产分组、漏洞处理状态（已处理、未处理）或输入服务器IP或名称定位到相关的漏洞影响资产。



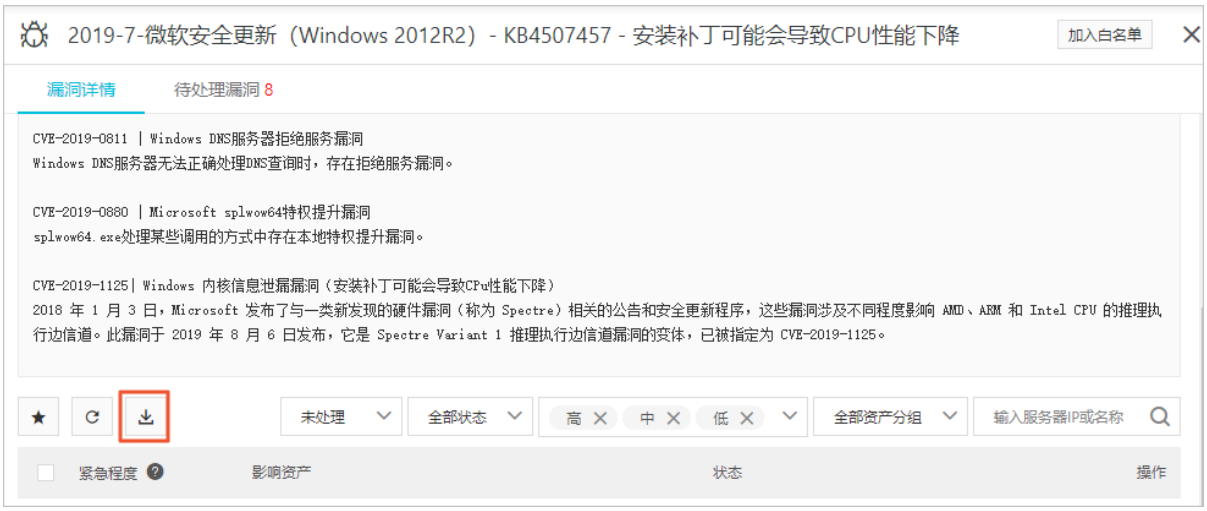
> **说明:**

搜索服务器IP或名称支持模糊查询。

- 导出漏洞影响资产

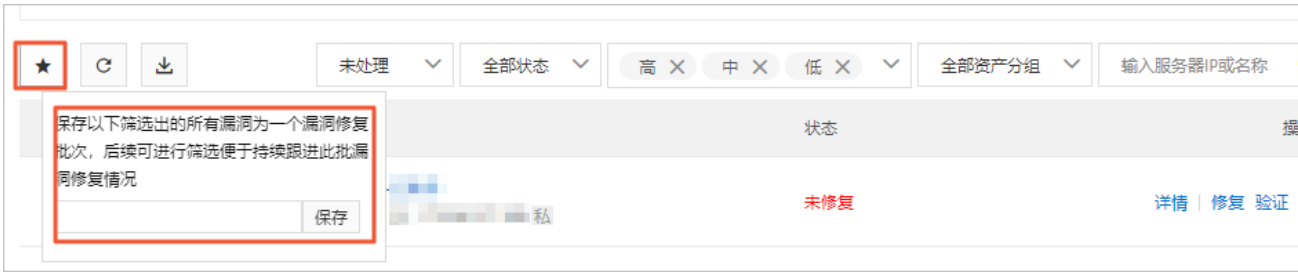
  您可在漏洞详情页面，单击导出按钮，将云安全中心检测到的该Linux系统漏洞下影响资产统一导出并保存到本地。导出的文件为Excel格式。

  说明:
  根据您资产中漏洞数据的大小，导出漏洞列表可能需要耗费一定时间，请耐心等待。



- 保存已筛选漏洞

  您可在漏洞详情页面，单击  按钮保存筛选出的所有漏洞为一个漏洞修复批次，方便您对该批次漏洞的状态进行持续跟踪。



相关文档

#unique_10

1.4 Web-CMS漏洞

云安全中心支持检测并快速修复Web-CMS漏洞。可监控网站目录，识别通用建站软件，通过漏洞文件比对方式检测建站软件中的漏洞。

背景信息

Web-CMS漏洞功能通过及时获取最新的漏洞预警和相关补丁，并通过云端下发补丁更新，实现漏洞快速发现、快速修复的功能。云安全中心Web-CMS漏洞功能帮助您解决漏洞发现不及时、不会修复漏洞、无法批量进行补丁更新等诸多问题。

说明:

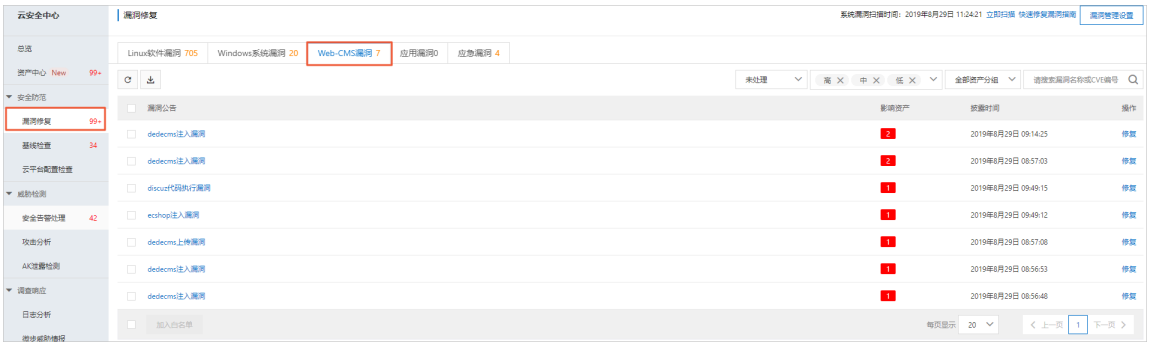
- 云安全中心基础版只提供Web-CMS漏洞检测，不提供漏洞修复的服务；如需一键修复漏洞，请开通云安全中心高级版或企业版。基础版、高级版和企业版详细功能介绍参见#unique_6。
- Web-CMS漏洞修复后立即生效，无需再次验证。

查看漏洞基本信息

1. 登录云安全中心控制台。
2. 在左侧导航栏，单击安全防范 > 漏洞修复，打开漏洞修复页面，单击Web-CMS漏洞。

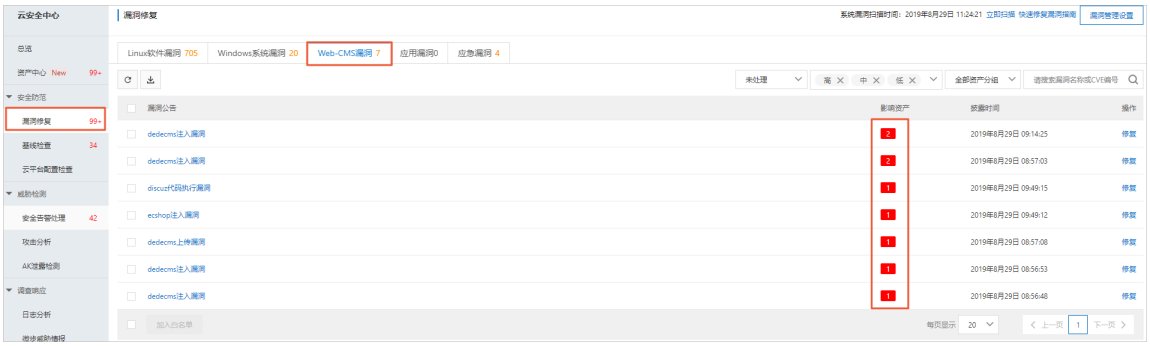
3. 在Web-CMS漏洞页面，查看和管理云安全中心检测到的所有Web-CMS漏洞信息。

- 查看漏洞信息



- 查看漏洞的修复紧急度建议

Web-CMS类型漏洞已经过工程师确认可导致严重危害，因此所有检查出的Web-CMS漏洞修复紧急度都为高，并用红色图标表示。

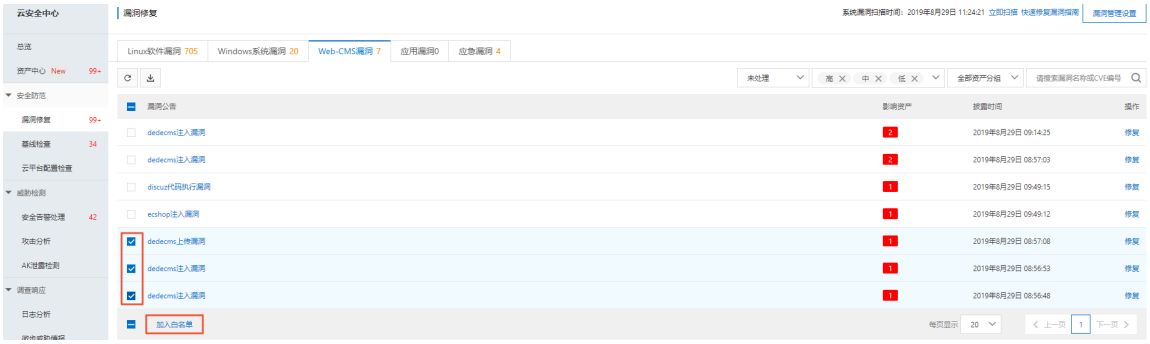


说明:

Web-CMS类型漏洞建议尽快修复。

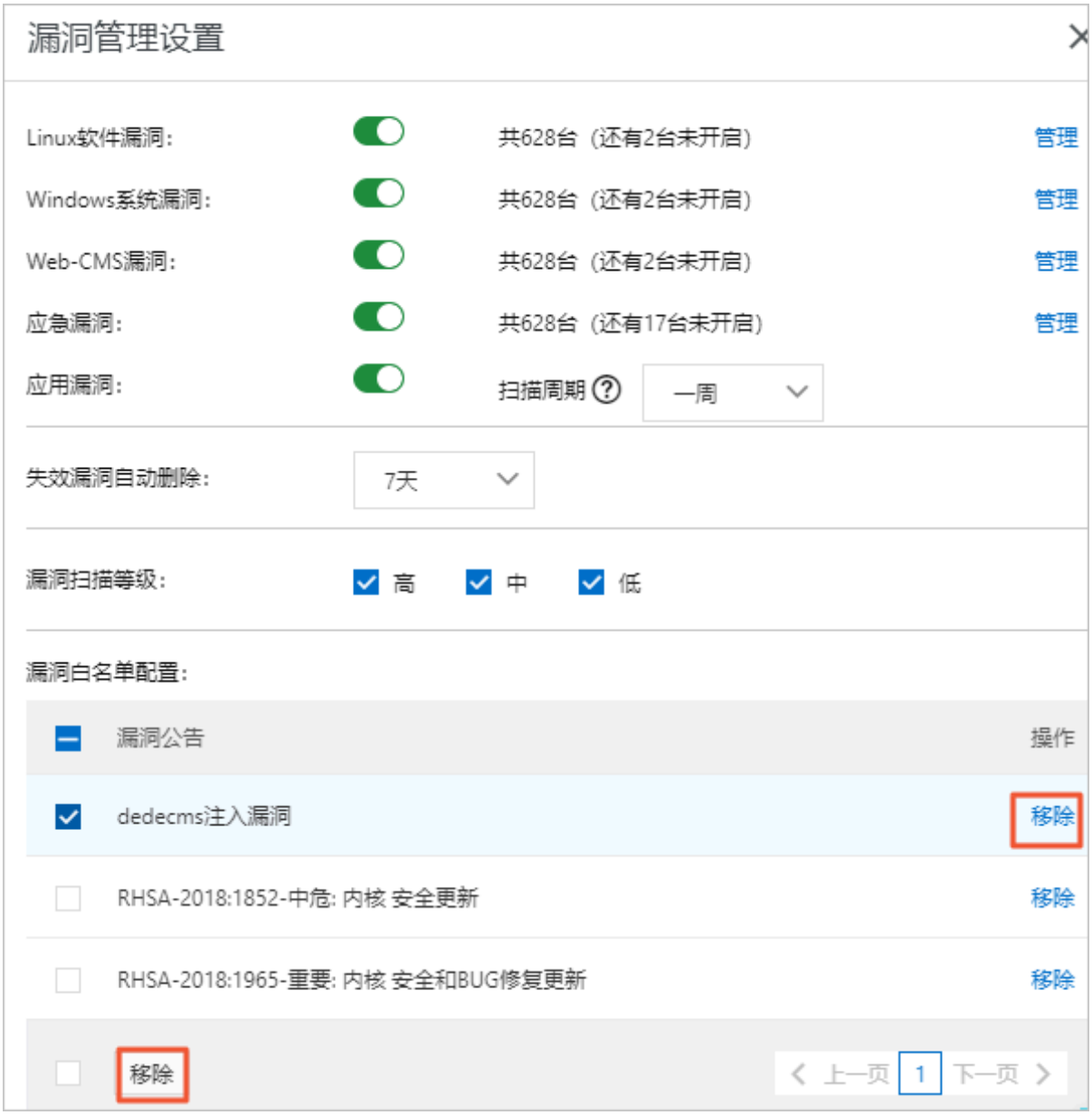
- **将漏洞加入白名单**

  您可在Web-CMS漏洞页面，勾选漏洞列表左侧的复选框后，单击加入白名单，将该漏洞加入白名单中。加入白名单后，云安全中心将不再对白名单中的漏洞进行告警。



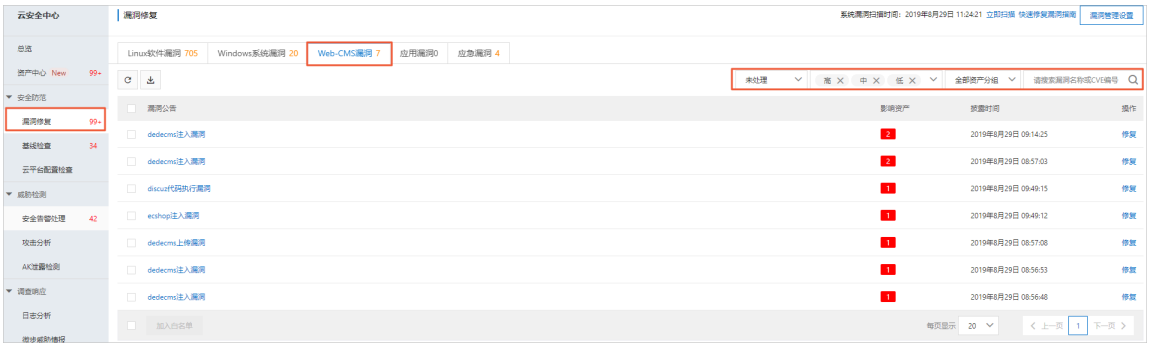
加入白名单的漏洞将从Web-CMS漏洞的漏洞列表中移除，并记录在漏洞管理设置页面的漏洞白名单配置列表中。

如需恢复云安全中心对白名单中的漏洞进行检测和告警提示，可在漏洞管理设置页面移除该漏洞。



- **搜索漏洞**

  您可在Web-CMS漏洞页面，通过筛选漏洞危险等级（高、中、低）、漏洞处理状态（已处理、未处理）、资产分组或输入漏洞名称定位到相关的漏洞。

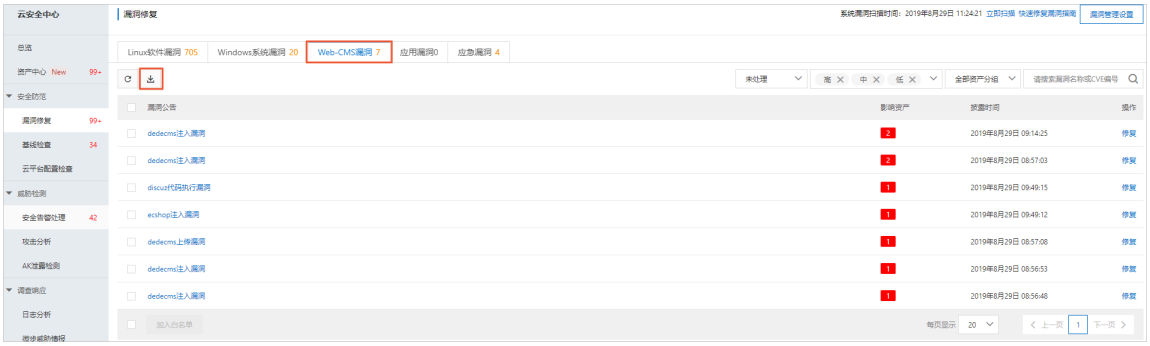


> **说明:**
> 搜索漏洞名称支持模糊查询。

- 导出漏洞

  您可在Web-CMS漏洞页面，单击导出按钮，将云安全中心检测到的所有Linux系统漏洞统一导出并保存到本地。导出的文件为Excel格式。

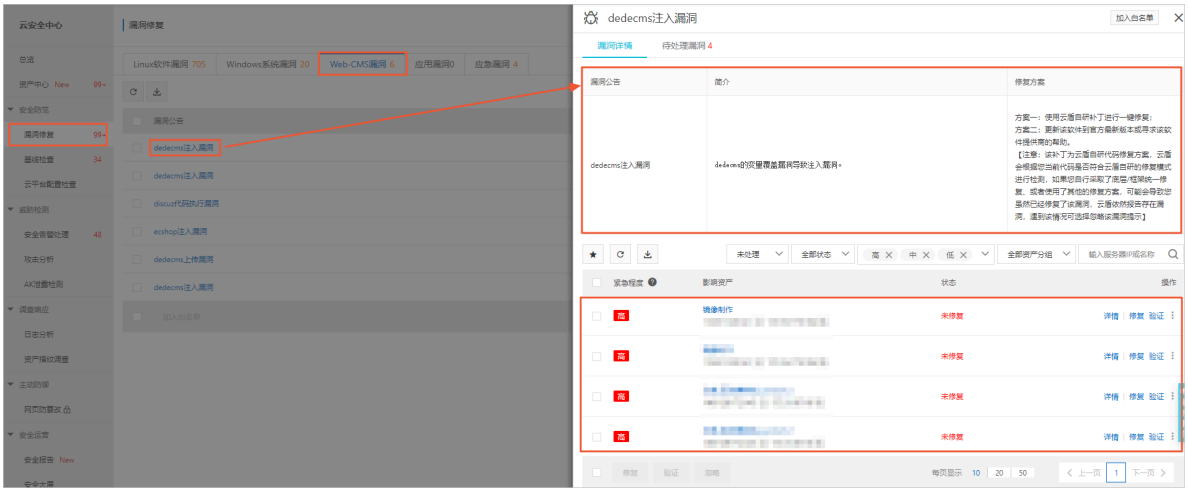
> **说明:**
> 根据您资产中漏洞数据的大小，导出漏洞列表可能需要耗费一定时间，请耐心等待。



查看漏洞详情和处理漏洞

1. 登录云安全中心控制台。
2. 在左侧导航栏，单击安全防范 > 漏洞修复，打开漏洞修复页面，单击Web-CMS漏洞。
3. 在漏洞列表，单击漏洞公告名称或漏洞公告对应操作栏下的修复，可展开对应的漏洞详情页面。

   您可查看该漏洞的漏洞详情、待处理漏洞数量及关联资产信息。



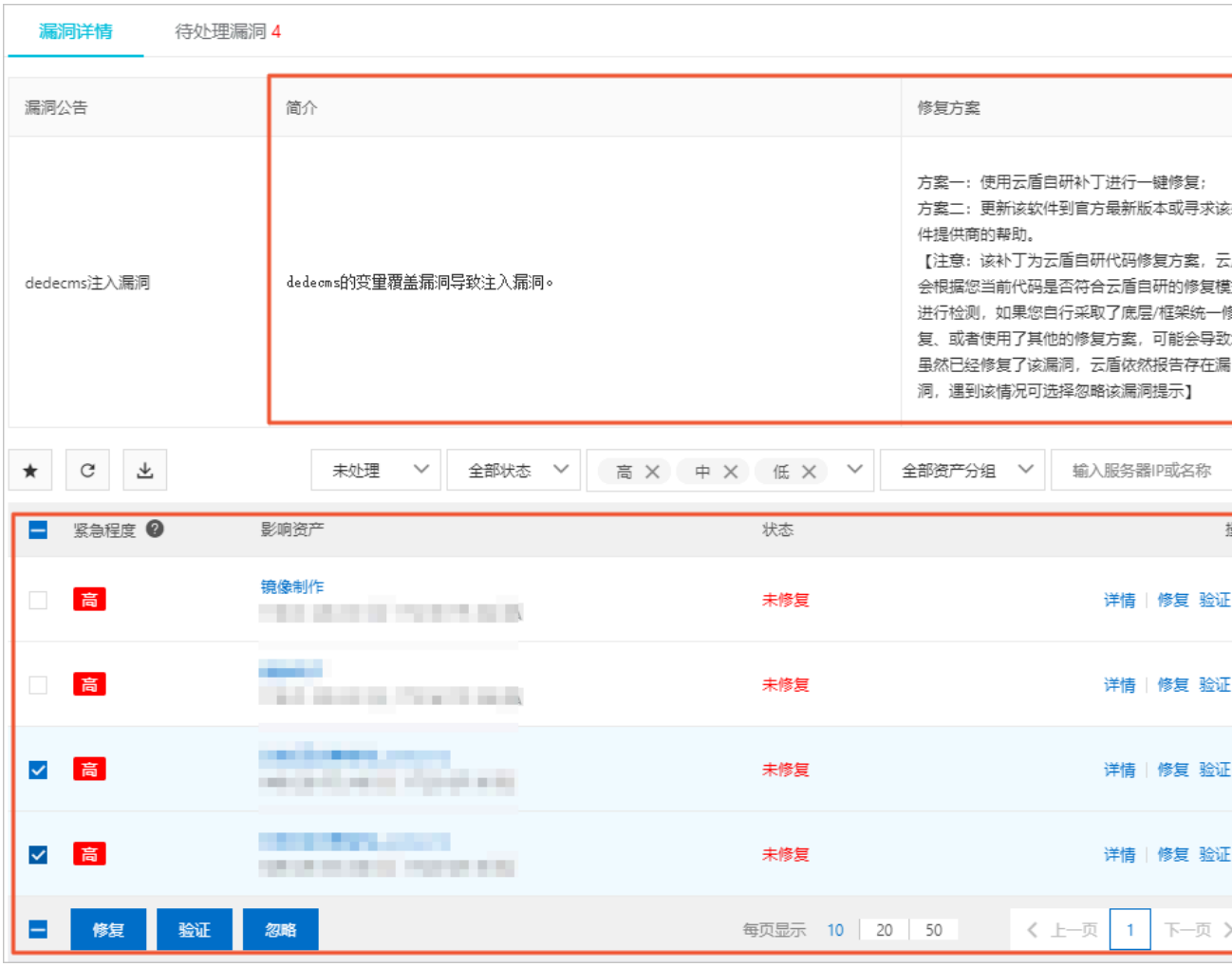
4. 在漏洞详情页面，您可以根据需要执行以下步骤管理漏洞详情。

· 查看漏洞详情

漏洞详情页面可展示该漏洞所有关联漏洞，即该漏洞影响的所有资产信息，方便您对所有相关的漏洞进行分析和批量处理。

- 单击漏洞详情页签，您可在漏洞详情子页查看该漏洞公告简介和修复方案。
- 单击待处理漏洞页签，直接跳至漏洞详情下的漏洞影响资产列表。

  您可在漏洞影响资产列表，查看该漏洞影响的所有资产、漏洞的状态等信息，并可对漏洞执行验证、修复、加入白名单或忽略的操作。



在漏洞详情页面的漏洞列表中，单击漏洞影响列表的影响资产名称可定位到资产中心 > 漏洞信息页面，为您展示该资产关联的所有Web-CMS漏洞信息。

- **查看漏洞的修复紧急度建议**

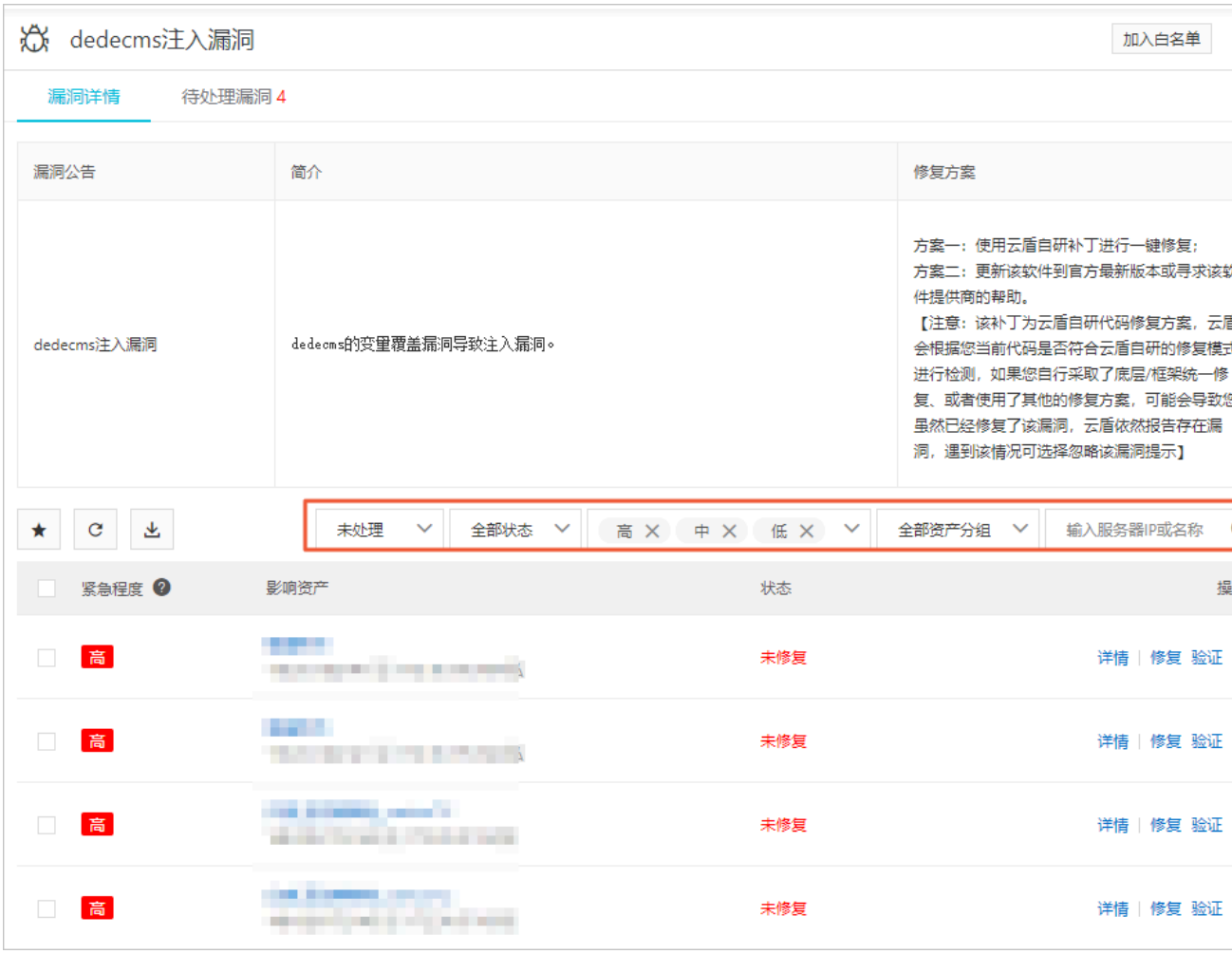
  Web-CMS类型漏洞已经过工程师确认可导致严重危害，因此所有检查出的Web-CMS漏洞修复紧急度都为高，并用红色图标表示。

说明：

Web-CMS类型漏洞建议尽快修复。

- 搜索漏洞

您可在漏洞详情页面，通过筛选漏洞危险等级（高、中、低）、资产分组、漏洞处理状态（已处理、未处理）或输入服务器IP或名称定位到相关的漏洞影响资产。



说明:

搜索服务器IP或名称支持模糊查询。

- 查看漏洞详细状态
  - 已处理
    - 修复成功：漏洞已执行一键修复并修复成功。
    - 修复失败：漏洞修复失败，可能因为漏洞文件已被修改或漏洞文件已不存在。
    - 已忽略：漏洞已执行忽略的操作，云安全中心将不再对该漏洞进行告警。
    - 漏洞已失效：表示该漏洞在7天内未被再次扫描到。
    - 回滚失败：漏洞回滚失败、无法回到未处理状态，可能因为漏洞文件已不存在。

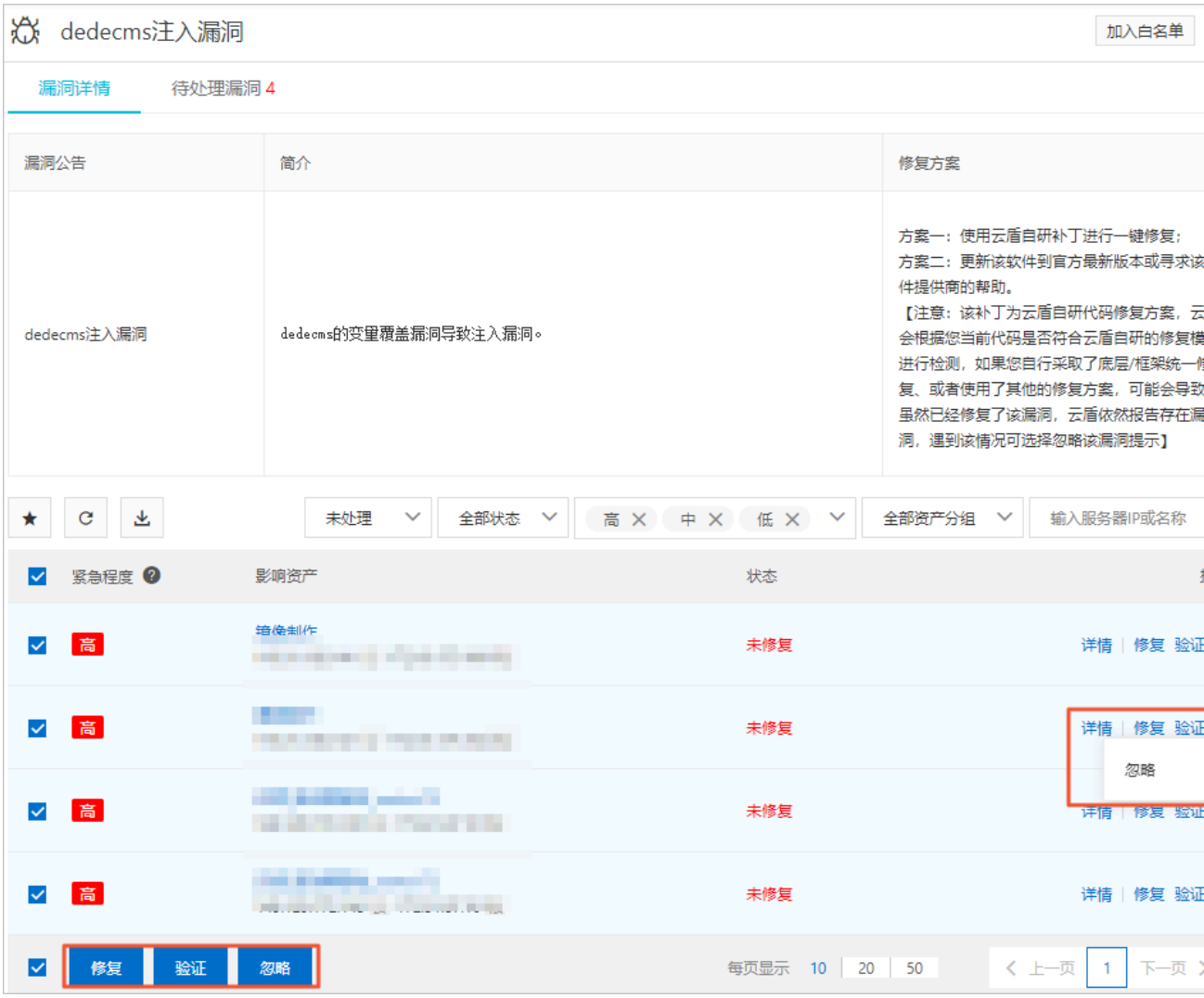
 说明：

已处理的漏洞支持回滚操作，漏洞回滚后将重新变为未处理的状态。

- 未处理：未修复，即漏洞待修复。

· 处理受影响资产漏洞

您可对受影响资产漏洞进行修复、验证、加白名单或忽略的操作。



- 修复漏洞

  您可在漏洞详情页面，单击修复，单个修复漏洞或批量修复多个关联漏洞。

- 验证漏洞：Web-CMS漏洞修复后立即生效，无需再次验证。

- 将漏洞加入白名单

  您可在漏洞详情页面，单击右上角加入白名单，将该漏洞加入白名单中。加入白名单后，云安全中心将不再对白名单中的漏洞进行告警。

  加入白名单的漏洞将从漏洞列表中移除，并记录在漏洞管理设置页面的漏洞白名单配置列表中。

如需恢复云安全中心对白名单中的漏洞进行检测和告警提示，可在漏洞管理设置页面移除该漏洞。

- 忽略漏洞

  您可在漏洞详情页面，勾选漏洞列表左侧的复选框后，单击并选择忽略，云安全中心将不再提示该漏洞。

  > 说明:
  > 被忽略的漏洞状态将转为已忽略。如需云安全中心继续对该漏洞进行告警提示，可在已处理的漏洞列表中找到该漏洞并对其取消忽略。

- 回滚漏洞

  云安全中心支持对已处理的漏洞，进行回滚操作，漏洞回滚后将重新变为未处理的状态。

· 导出漏洞影响资产

您可在漏洞详情页面，单击导出按钮 ，将云安全中心检测到的该漏洞下影响资产统一导出并保存到本地。导出的文件为Excel格式。

> 说明:

根据您资产中漏洞数据的大小，导出漏洞列表可能需要耗费一定时间，请耐心等待。

- 保存已筛选漏洞

  您可在漏洞详情页面，单击  按钮，保存筛选出的所有漏洞为一个漏洞修复批次，方便您对该批次漏洞的状态进行持续跟踪。

1.5 应用漏洞

云安全中心企业版支持应用漏洞检测，可检测主流的应用漏洞类型。

背景信息

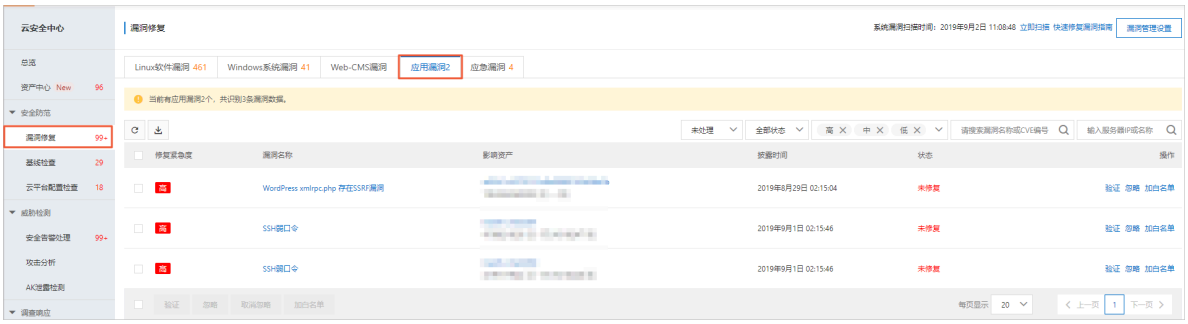
应用漏洞为企业版功能，基础版和高级版不支持。基础版和高级版用户需先升级到企业版，才可使用应用漏洞功能。

操作步骤

1. 登录云安全中心控制台。

2. 在左侧导航栏，单击安全防范 > 漏洞修复，打开漏洞修复页面，单击应用漏洞。

3. 在应用漏洞页面，查看云安全中心检测到的所有应用漏洞，查看漏洞修复建议、严重程度和状态及处理漏洞。

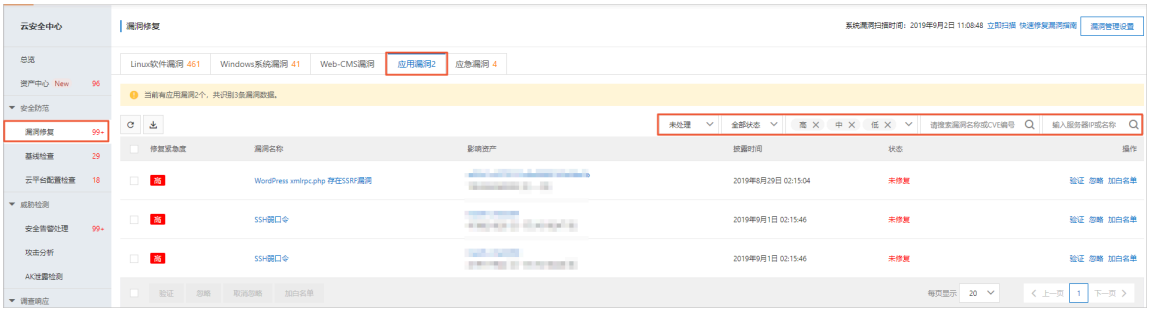


- 查看漏洞的修复紧急度建议

  应用漏洞紧急程度分为高（红色图标表示）、中（橙色图标表示）、低（灰色图标表示）三类。

- 查看漏洞详细状态
  - 已处理
    - 修复成功：该应用漏洞已成功修复。
    - 修复失败：漏洞修复失败。
    - 已忽略：漏洞已执行忽略的操作，云安全中心将不再对该漏洞进行告警。
    - 漏洞已失效：表示该漏洞在7天内未被再次扫描到。
  - 未处理：未修复，即漏洞待修复。
- 搜索漏洞

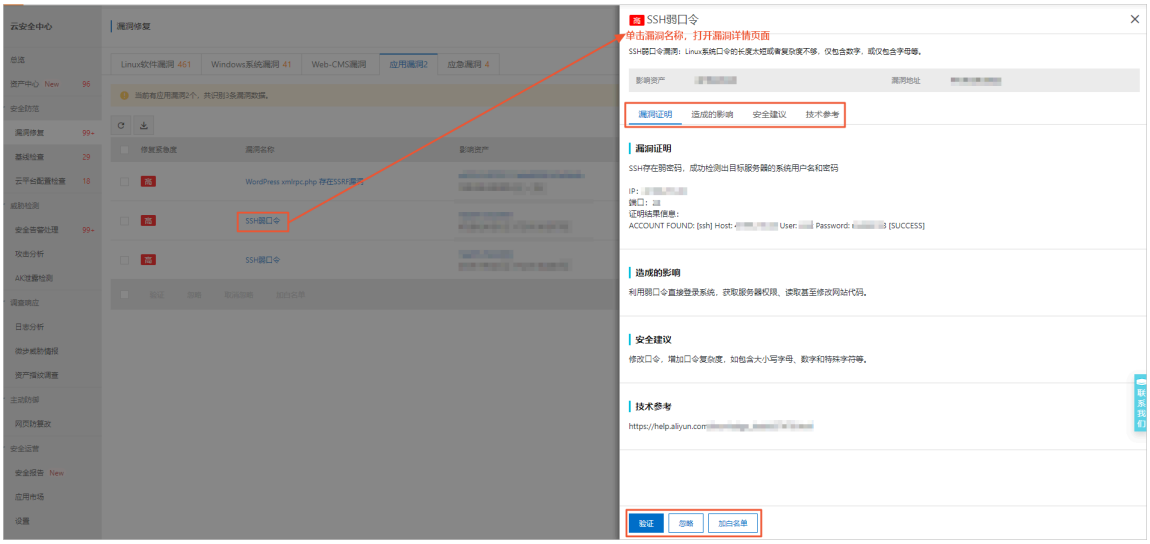
  您可在应用漏洞页面通过筛选漏洞危险等级（高、中、低）、漏洞处理状态（已处理、未处理）、搜索漏洞名称或输入服务器IP/名称定位到相关的漏洞。



- 查看漏洞详情

  在应用漏洞页面，单击漏洞列表中漏洞名称列的目标漏洞名称，打开该漏洞详情页面。

  您可在漏洞详情页面，查看该漏洞的受影响资产信息、漏洞证明、安全建议等信息，并可执行忽略漏洞、将漏洞加入白名单、验证漏洞等操作。



在应用漏洞页面，单击漏洞列表中影响资产列的目标资产名称，可定位到资产列表 > 漏洞信息 > 应用漏洞页面，了解该资产中检测到的应用漏洞信息。

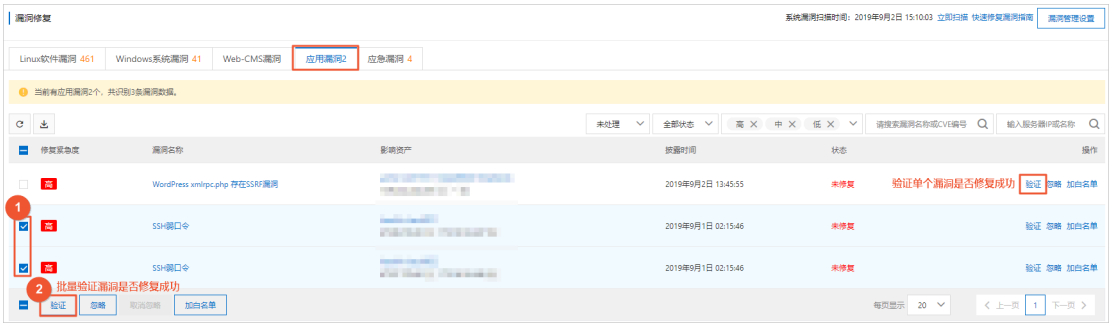
- 处理漏洞
  - 修复漏洞

    您可在漏洞详情页面，查看漏洞安全建议，对漏洞进行相应的修复操作。

- **验证漏洞**

  ■ 您可在指定漏洞的详情页面下方，单击验证，检测该漏洞是否已修复成功。

  ■ 您也可在应用漏洞页面，批量验证漏洞，检测漏洞是否已修复成功。

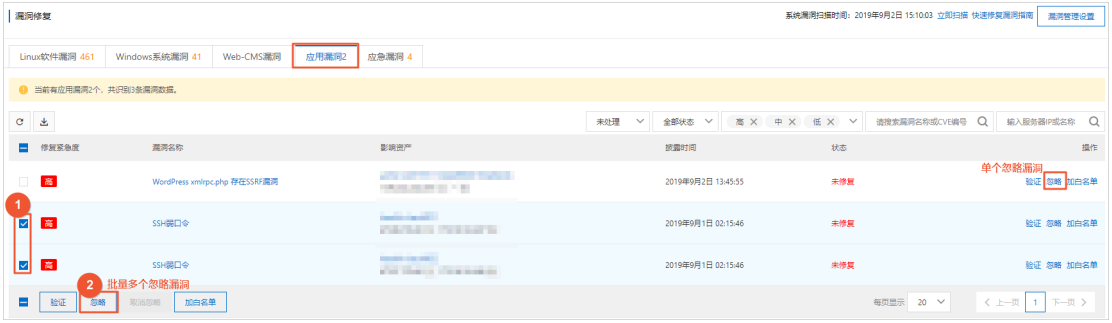


单击验证后，该漏洞的状态转为验证中。需要等待数秒后漏洞验证才可完成。

- 忽略漏洞

  ■ 您可在指定漏洞的详情页面下方，单击忽略，云安全中心将不再提示该漏洞。

  ■ 您也可在应用漏洞页面，批量忽略漏洞，云安全中心将不再提示忽略的漏洞。



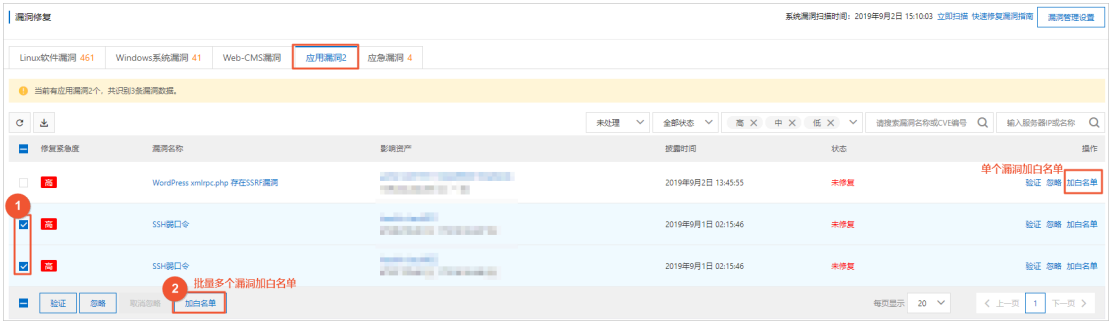
说明:

被忽略的漏洞状态将转为已忽略。如需云安全中心继续对该漏洞进行告警提示，可在已处理的漏洞列表中找到该漏洞并对其取消忽略。

- 将漏洞加入白名单

  ■ 您可在指定漏洞的详情页面下方，单击加白名单，将该漏洞加入白名单中。

  ■ 您也可在应用漏洞页面，将单个或批量多个漏洞加入白名单。



对于加入白名单的应用漏洞，云安全中心将不再对白名单中的应用漏洞进行告警。

加入白名单的漏洞将从漏洞列表中移除，并记录在漏洞管理设置页面的漏洞白名单配置列表中。

如需恢复云安全中心对白名单中的漏洞进行检测和告警提示，可在漏洞管理设置页面的漏洞白名单列表中移除该漏洞。

- 导出漏洞

  您可在应用漏洞页面，单击导出按钮，将云安全中心检测到的所有应用漏洞统一导出并保存到本地。导出的文件为Excel格式。

  说明:
  根据您资产中漏洞数据的大小，导出漏洞列表可能需要耗费一定时间，请耐心等待。

支持检测的应用漏洞

应用漏洞类型	检测项
系统服务弱口令	OpenSSH 服务
	MySQL 数据库服务
	MSSQL 数据库服务
	MongoDB 数据库服务
	FTP/VSFTP/ProFTPD 服务
	Memcache 缓存服务
	Redis 缓存服务

应用漏洞类型	检测项
	Subversion 版本控制服务
	SMB 文件共享服务
	SMTP 邮件发送服务
	POP3 邮件接收服务
	IMAP 邮件管理服务
系统服务漏洞	OpenSSL 心脏滴血
	SMB · Samba · 弱口令暴力破解
	RSYNC · 匿名访问导致敏感文件信息 · 认证密码暴力破解
	VNC 密码暴力破解
	pcAnywhere 密码暴力破解
	Redis 密码暴力破解
应用服务漏洞	phpMyAdmin 弱口令检测
	Tomcat 控制台弱密码检测
	Apache Struts 2 远程命令执行漏洞
	Apache Struts 2 远程命令执行漏洞（S2-046）
	Apache Struts 2 远程命令执行漏洞（S2-057）
	ActiveMQ CVE-2016-3088 任意文件上传漏洞
	Confluence 任意文件读取漏洞
	CouchDB Query Server 远程命令执行
	Discuz! 后台管理员弱口令破解
	Docker 未授权访问漏洞
	Drupal Drupalgeddon2 远程代码执行CVE-2018-7600
	ECshop 登录接口代码执行漏洞
	Elasticsearch 未授权访问
	Elasticsearch MvelRCE CVE-2014-31
	Elasticsearch Groovy RCE CVE-2015-1427

应用漏洞类型	检测项
	泛微OA表达式注入
	Hadoop YARN ResourceManager 未授权访问
	JavaServer Faces 2 目录遍历漏洞
	JBoss EJBInvokerServlet Java 反序列化漏洞
	Jenkins Manage 匿名访问CVE-2018-1999001 CVE-2018-1999002
	Jenkins 未授权访问
	Jenkins Script Security Plugin RCE
	Kurbernetes 未授权访问漏洞
	MetInfo getPassword 接口存在SQL注入漏洞
	MetInfo login 接口存在SQL注入漏洞
	PHPCMS 9.6 任意文件上传漏洞
	PHP-CGI 远程代码执行
	Actuator unauth RCE
	ThinkPHP_RCE_20190111
	WebLogic UDDI Explorer SSRF 漏洞
	WordPress xmlrpc.php 存在SSRF漏洞
	Zabbix Web 控制台暴力破解
	OpenSSL 心脏滴血检测
	Apache Tomcat WEB-INF 配置文件未授权访问

1.6 应急漏洞

云安全中心支持对互联网上突然出现的紧急漏洞进行检测和修复。

背景信息

云安全中心应急漏洞页面会展示近期爆发出的高危漏洞，您可通过云安全中心漏洞管理提供的检测功能对您的资产进行实时检测，确认是否有资产受到影响。

说明:

基础版、高级版和企业版都支持应急漏洞功能。

云安全中心提供的应急漏洞功能具有以下特性：

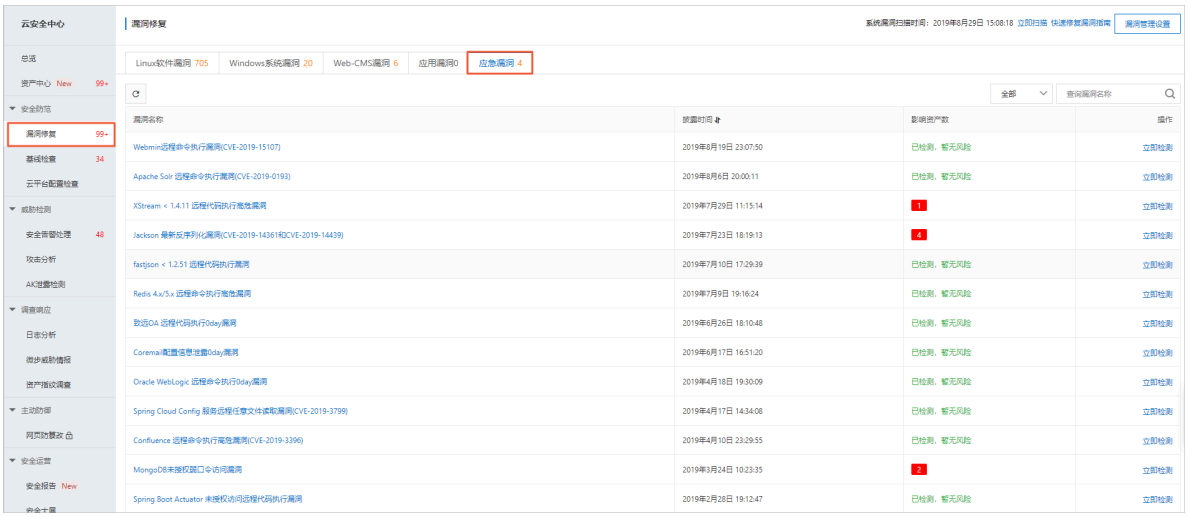
- 应急漏洞披露时间支持排序

- 支持应急漏洞检测与告警
- 实时展示应急漏洞检测进度
- 实时展示应急漏洞影响的资产数量并提供漏洞详情信息
- 实时展示应急漏洞的修复紧急程度
- 对检测出的应急漏洞提供修复建议
- 支持应急漏洞修复完成后进行验证，确认该漏洞是否已成功修复

查看漏洞基本信息

1. 登录云安全中心控制台。
2. 在左侧导航栏，单击安全防范 > 漏洞修复，打开漏洞修复页面，单击应急漏洞。

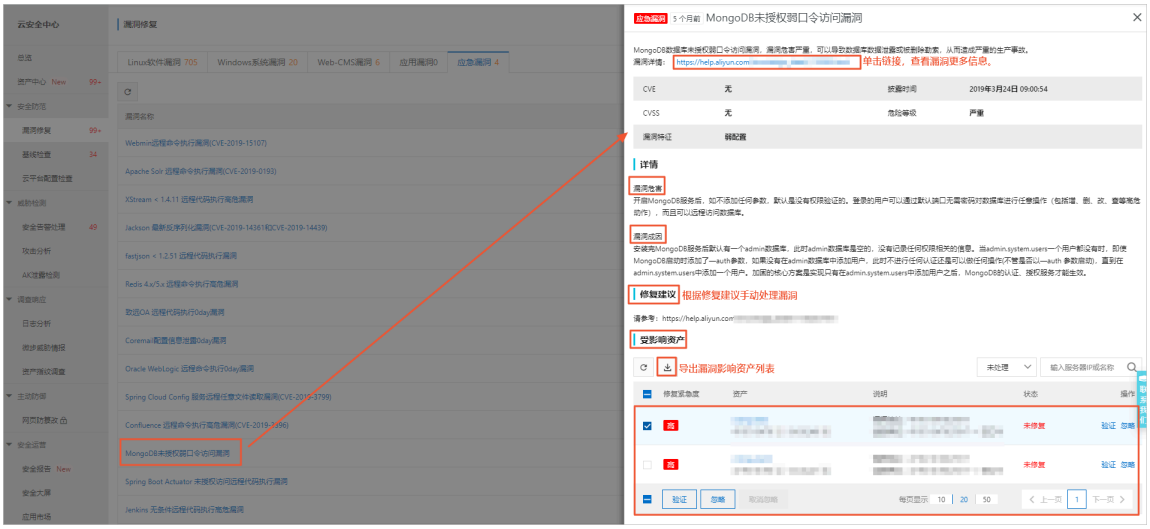
3. 在应急漏洞页面，查看云安全中心检测到的最新应急漏洞情况和应急漏洞记录，并对应急漏洞进行检测，确认该漏洞是否对您的资产有影响。



- 检测漏洞

  在漏洞列表中，单击待检测漏洞右侧的立即检测，对应急漏洞执行检测。

  如果有检测到风险，云安全中心会在影响的资产数红色高亮显示，并展示检测到存在该应急漏洞的资产数量。您可单击该应急漏洞名称前往漏洞详情页面，查看漏洞具体信息，并对该漏洞进行处理。



说明：

对于从未被检测过的漏洞，会在影响资产数一栏中提示未检测。

- 查看漏洞检测进度

  单击立即检测后，云安全中心会为您实时展示该应急漏洞的检测进度。

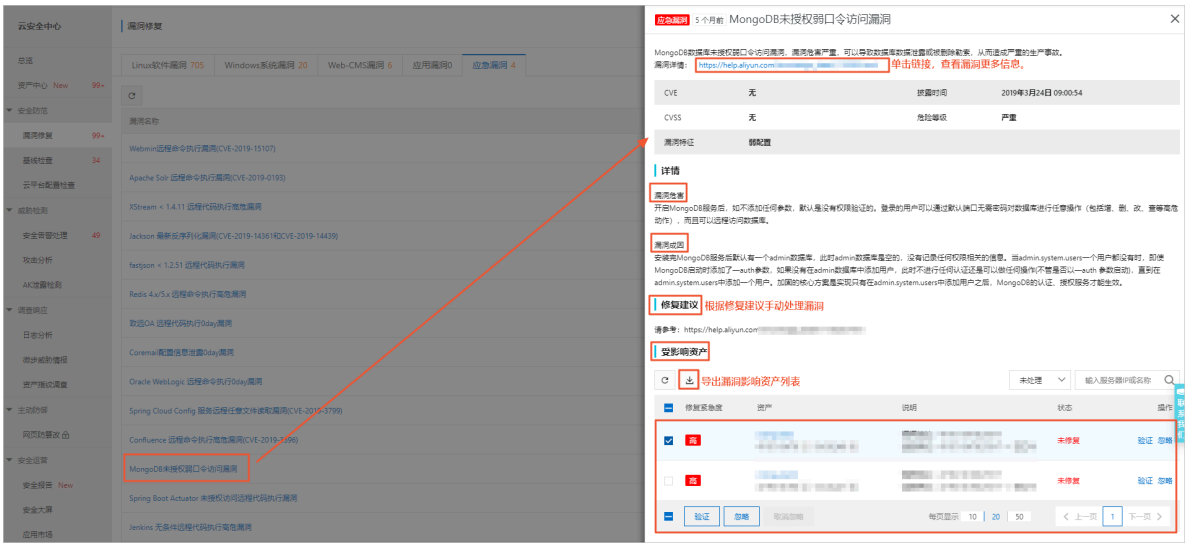
- 搜索漏洞

  您可在应急漏洞页面，通过筛选漏洞风险状态（存在风险、无风险）或输入漏洞名称定位到相关的漏洞。

查看漏洞详情和处理漏洞

1. 登录云安全中心控制台。
2. 在左侧导航栏，单击安全防范 > 漏洞修复，打开漏洞修复页面，单击应急漏洞。

3. 单击漏洞名称，跳转到漏洞的详情页面，查看应急漏洞的详细信息、影响的资产、修复必要性和部分漏洞的修复建议，并处理漏洞。



您可在应急漏洞详情页面，查看该应急漏洞影响的资产信息，并根据修复建议处理漏洞。

- 查看受影响资产的漏洞详细状态
  - 已处理
    - 修复成功：漏洞已成功修复。
    - 修复失败：漏洞修复失败，可能因为漏洞文件已被修改或漏洞文件已不存在。
    - 已忽略：漏洞已执行忽略的操作，云安全中心将不再对该漏洞进行告警。
    - 漏洞已失效：表示该漏洞在7天内未被再次扫描到。
    - 回滚失败：漏洞回滚失败、无法回到未处理状态，可能因为漏洞文件已不存在。

    说明：
    已处理的漏洞支持回滚操作，漏洞回滚后将重新变为未处理的状态。
  - 未处理：未修复，即漏洞待修复。
- 查看受影响资产的漏洞修复紧急度。

  漏洞修复紧急度是根据漏洞等级、公开时间、服务器真实环境等因素综合分析出来的修复建议说明。

  漏洞修复必要性分为高、中、低三个等级。

  说明：

建议立即对高修复紧急度的漏洞立即修复。

- 处理受影响资产的应急漏洞
  - 根据漏洞详情页面提示的漏洞修复建议，在受影响的资产中手动进行修复。
  - 验证：验证漏洞是否已修复成功。
  - 忽略：忽略漏洞，云安全中心本次将不再提示该漏洞。

> 说明:
> 被忽略的漏洞，状态将转为已忽略。如需云安全中心继续对该漏洞进行告警提示，可在已处理的漏洞列表中，找到该漏洞并对其取消忽略。

- 导出漏洞影响资产

  您可在漏洞详情页面，单击导出按钮  ，将云安全中心检测到的该漏洞下影响资产统一导出并保存到本地。导出的文件为Excel格式。

> 说明:
> 根据您资产中漏洞数据的大小，导出漏洞列表可能需要耗费一定时间，请耐心等待。

1.7 漏洞管理设置与加白名单

您可通过漏洞管理设置开启/关闭不同类型漏洞的自动检测、有选择性地对指定服务器开启漏洞检测、对已失效漏洞设置自动删除周期、或配置漏洞白名单。

您可以在Linux软件漏洞、Windows系统漏洞、Web-CMS漏洞、应用漏洞列表中批量添加漏洞至白名单。添加成功后，系统将不再检测漏洞白名单中的漏洞。您可以通过漏洞管理设置对漏洞白名单进行维护。

操作步骤

1. 登录云安全中心控制台。
2. 单击安全防范 > 漏洞修复 > 漏洞管理设置。

3. 在漏洞管理设置页面，可执行以下操作：

- 单击漏洞类型右侧的切换开关，开启/关闭该漏洞检测。
- 单击管理，添加开启该漏洞检测的服务器。
- 设置失效漏洞自动删除周期：7天、30天、90天。

> **说明：**
> 对于检测出来的漏洞如果不做任何处理，默认该告警失效；失效漏洞将在指定周期后自动从漏洞列表中移除。

- 在漏洞白名单配置列表中勾选相应漏洞，单击移除，重新启用对该漏洞的检测和告警。

1.8 服务器软件漏洞修复

本文介绍了修复服务器软件漏洞的最佳实践方法。

当云安全中心的主机漏洞功能发现您服务器上的漏洞后，您可参考以下方法来修复服务器上的漏洞，保证漏洞修复工作的有效性和可靠性。

> **说明：**
> 本方法适用于服务器上的各类操作系统、网络设备、数据库、中间件的漏洞修复工作。

服务器软件漏洞修复方法

不同于普通PC上的漏洞修复，服务器上的软件漏洞修复应由具备一定专业知识的人员进行操作。漏洞修复工作的负责人应遵循以下修复流程：

修复前

1. 修复人员应对目标服务器系统进行资产确认，并通过云安全中心对目标服务器系统上的系统漏洞进行确认。关于云安全中心对Linux软件漏洞的各项参数说明，请参考Linux软件漏洞参数说明。
2. 修复人员在确认目标服务器上的系统漏洞后，应确认哪些系统漏洞需要修复。并不是所有被发现的软件漏洞都需要在第一时间进行修复，应根据实际业务情况、服务器的使用情况、及漏洞修复可能造成的影响来判定漏洞是否需要修复。
3. 修复人员在测试环境中部署待修复漏洞的相关补丁，从兼容性和安全性方面进行测试，并在测试完成后形成漏洞修复测试报告。漏洞修复测试报告应包含漏洞修复情况、漏洞修复的时长、补丁本身的兼容性、及漏洞修复可能造成的影响。
4. 为了防止出现不可预料的后果，在正式开始漏洞修复前，修复人员应使用备份恢复系统对待修复的业务服务器系统进行备份。例如，通过ECS的快照功能备份目标ECS实例。

修复中

1. 在目标服务器部署修复漏洞的相关补丁及进行修复操作时，应至少有两名修复人员在场（一人负责操作，一人负责记录），尽量防止可能出现的误操作。
2. 修复人员按照待修复的系统漏洞列表，逐项进行升级、修复。

修复后

1. 修复人员对目标服务器系统上的漏洞修复进行验证，确保漏洞已修复且目标服务器没有出现任何异常情况。
2. 修复人员对整个漏洞修复过程进行记录，形成最终漏洞修复报告，并将相关文档进行归档。

服务器软件漏洞补丁修复风险规避措施

为了确保在服务器软件漏洞修复过程中目标服务器系统的正常运行、并将异常情况发生的可能性降到最低，在漏洞修复过程中应采取以下风险规避措施：

- 制定漏洞修复方案

  漏洞修复负责人应对修复对象（目标服务器）运行的操作系统和应用系统进行调研，并制定合理的漏洞修复方案。漏洞修复方案应通过可行性论证，并得到实际环境的测试验证支持。漏洞修复实施工作应严格按照漏洞修复方案所确定的内容和步骤进行，确保每一个操作步骤都对目标业务服务器系统没有损害。

- 使用仿真测试环境

  通过使用仿真测试环境，对漏洞补丁修复方案进行验证，证明制定的漏洞补丁修复方案对待修复的在线业务系统没有损害。

  > 说明:
  > 仿真测试环境要求系统环境（操作系统、数据库系统）与在线业务系统完全一致，应用系统也与在线业务系统的版本一致，数据建议采用在线业务系统最近一次的全备份数据。

- 进行系统备份

  对整个业务系统进行完全备份，包括系统、应用软件和数据。备份完成后，应对系统备份的数据进行有效性恢复验证。通过系统备份，当发生系统环境异常或数据丢失时，可以及时对系统进行恢复，确保业务稳定。建议使用ECS的快照功能对业务系统进行快速、高效的备份。

1.9 漏洞修复优先级排序参考

漏洞修复中的难点

保护您的云上资产安全最重要的环节包括对漏洞修复进行优先级评定。如果您拥有的资产数量较多，您会在控制台看到多个漏洞，您将需要考虑优先修复哪些漏洞。为了解决这个问题，我们提供了一套新颖的评价标准来为您有序地修复漏洞提供参考。

漏洞修复建议分数判定级别说明

- 修复紧急度高

  漏洞修复建议参考分在13.5-15之间。

- 修复紧急度中

  漏洞修复建议参考分在7.1-13.5之间。

- 修复紧急度低

  漏洞修复建议参考分在7以下。

漏洞修复建议参考分计算方法

最终风险得分 = 漏洞的CVSS得分 * 时间因子 * 用户实际环境因子 * 资产重要性因子

> 说明:
> 应急漏洞和Web-CMS漏洞均为经工程师反复确认的高危漏洞，所以统一建议您尽快修复。以下计算方式均只针对Linux软件漏洞和Windows系统/应用漏洞。

- 在计算漏洞修复建议得分的过程中，从新发现一个漏洞到控制台提供修复建议大约有1天的延迟。
- 漏洞刚被公布时，官方可能没有给出CVSS基础分，这一部分漏洞的修复建议将会延迟到官方给出CVSS分一天后才能为您显示。
- 由于您的Agent离线等其他网络异常问题也可能导致环境因子无法计算，此时您需要等待网络环境恢复正常后一天才能看到修复建议。

软件漏洞的CVSS基础分

这个因子来源于该漏洞的CVSS V2和V3基础分。

影响漏洞带来风险的时间因素

时间因子是为了弥补CVSS分的不足，综合了漏洞缓解措施被部署的时间延迟，和漏洞利用方法的普及因素的一条动态变化曲线。

在漏洞公开的前三天，由于曝光率的增加，该漏洞被利用的几率会急剧增加，时间因子将会达到短暂的峰值，随后急剧下降。 随着时间的推移，对漏洞成熟的利用手段将越来越多，漏洞实际利用难度在下降，时间因子将在100天之内逐渐趋近于1。

您的实际环境

您的实际环境对判断漏洞真实至关重要，我们对该漏洞利用所需的条件和您服务器的情况进行综合考虑，得出一个风险乘数。

当前纳入参考的环境因素有：

- 您的服务器是否有对公网的流量。

  如果是，且漏洞属于一个可以远程利用的漏洞，我们对环境因子进行1.5倍的加权；如果漏洞属于一个可邻网利用的漏洞，我们对环境因子进行1.2倍的加权；如果这个漏洞属于本地利用，我们不做加权；同时我们对某些需要云上难以复现的环境来利用的漏洞做环境因子大幅降权。
- 您的机器是否只有内网的流量。

  如果是，且漏洞属于一个可以远程利用的漏洞，我们对环境因子进行大幅降权（设0）；如果漏洞属于一个可邻网利用的漏洞，我们对环境因子进行1.2倍的加权；如果这个漏洞属于本地利用，我们不做加权；同时我们对某些需要云上难以复现的环境来利用的漏洞做环境因子大幅降权。

您的资产重要性

当您资产数量很多时，可以为不同的服务器或资产赋予您使用场景下的重要性分值，我们将把您自定义的分值纳入漏洞修复建议分的计算当中，为您有序修复漏洞提供有价值的参考。

说明:

资产重要性因子当前为 1。

特殊情况下的修复建议

- 当一个漏洞刚被扫描出来时，由于需要参照您的环境对参考分值进行加权，我们需要48小时的时间来评估修复建议，在这段时间内，漏洞的修复建议将按照漏洞本身的严重等级来给出：
  - 严重漏洞： 建议立即修复
  - 高危漏洞：可延后修复
  - 中危漏洞：可延后修复
  - 低危漏洞：暂可不修复
- 当由于网络抖动等原因我们无法获取该漏洞的环境因子时，该漏洞修复建议将统一为暂可不修复。

相关文档

- #unique_19
- 系统软件漏洞FAQ
- 系统软件漏洞各参数说明
- 如何手动检测系统软件漏洞

2 基线检查

2.1 基线检查概述

云安全中心企业版支持基线检查功能，对您的服务器安全配置进行检测并提供检测详情说明和基线加固建议。

功能描述

使用基线检查功能可自动检测服务器上的系统、账号、数据库、弱密码、合规性配置中存在的风险点，并提供加固建议。具体检测内容参见下方基线检测内容。

基线检查默认每天00:00-06:00进行一次全面的自动检测。支持用户自行添加和管理基线扫描策略，自定义需要检查的基线项目、检查周期、检测触发时间和应用该策略的服务器。

限制说明

基线检查功能为云安全中心的增值服务，仅企业版用户可开通和使用该服务。基础版和高级版用户都需先升级到企业版才可使用基线检查功能。

部分弱密码检测项（例如：MySQL弱密码检测、PostgreSQL弱密码检测、Microsoft SQLServer弱密码检测可能采用尝试登录的方式进行检测，从而会占用一定的服务器资源，产生较多的登录失败记录）和系统等保、CIS标准检测项默认关闭。如果您需要检查该项目，请确认上述风险后，在自定义基线扫描策略时勾选这些检测项目。

基线检测内容

基线检查项分类	检测项
数据库	检测Redis、Memcached高危监听配置风险以及启动权限配置风险。
系统	等保合规基线检查对标中国等保2.0第二/三等级保护基本要求的部分检查项目；安全基线检查对标阿里云、CIS标准： · Aliyun Linux 2等保合规基线检查和安全基线检查 · CentOS Linux 6/7等保合规基线检查和安全基线检查 · Ubuntu等保合规基线检查和阿里云标准安全基线检查 · Ubuntu 14/16 CIS标准安全基线检查 · Debian Linux 8等保合规基线检查和安全基线检查 · Windows 2008 R2、2012 R2、2016 R2和2019 R2等保合规检查和安全基线检查
弱密码检测	PostgreSQL弱密码检测
	Windows系统登录弱口令检测

基线检查项分类	检测项
	Microsoft SQL Server弱密码检测
	Linux系统登录弱口令检测
	MySQL弱密码检测
	FTP匿名登录配置检测
	FTP登录弱口令检测
中间件	阿里云标准-Apache Tomcat 安全基线检查

2.2 管理基线检查策略

本文档介绍了如何新增、编辑、删除基线检查策略，并设置基线检查等级的范围。

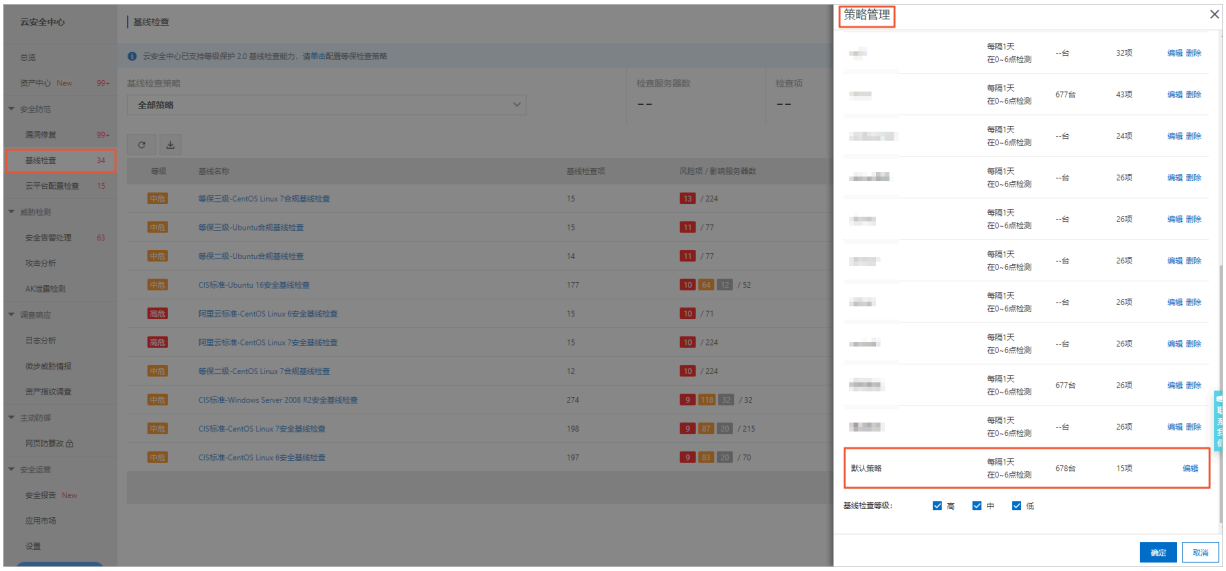
背景信息

基线检查功能为云安全中心的增值服务，仅企业版用户可开通和使用该服务。基础版和高级版用户都需先升级到企业版才可使用基线检查功能。

开通基线检查服务后，云安全中心将使用默认策略对所有资产进行检测。

默认策略自动检测时间：每天06:00-12:00

默认策略检测对象：您阿里云账号下的所有资产



您也可自定义基线检查策略，补充默认策略无法检测的基线项目。

操作步骤

1. 登录云安全中心控制台。
2. 在左侧导航栏，单击安全防范 > 基线检查。

3. 单击控制台界面右上角策略管理，自定义基线检查策略或修改默认策略。

- 在策略管理页面，单击策略列表左上角的新增策略，自定义基线扫描策略。

配置项	说明
策略名称	输入用于识别该模板的名称。
检测周期	选择检测周期（每隔1天/3天/7天/30天检测一次）和检测触发时间（00:00-06:00、06:00-12:00、12:00-18:00、18:00-24:00）。
基线名称	勾选需要检测的基线项目，在数据库、系统、弱密码检测、中间件下勾选具体需要检测的内容。 基线检查项目详情参见基线检查内容表。
生效服务器	勾选需要应用该策略的分组资产。 说明: 新购买的服务器默认归属在分组资产 > 未分组中，如需对新购资产自动应用该策略，请勾选未分组。

- 在策略管理页面，单击目标策略模板后的编辑或删除，对已有策略进行修改或删除。

说明:
策略删除后不可恢复。

- 在策略管理页面，单击策略模板列表中默认策略右侧操作栏下的编辑，调整应用默认策略的资产分组。

说明:

默认策略不支持删除、检测项不支持更改，仅支持修改应用默认策略的资产分组。

- **在策略管理页面下方，您可以设置基线检查的等级范围（高、中、低）。**

2.3 执行基线检测

本文档介绍了如何对基线策略执行检测，并查看检测结果和基线加固建议。

背景信息

基线检查功能为云安全中心的增值服务，仅企业版用户可开通和使用该服务。基础版和高级版用户都需先升级到企业版才可使用基线检查功能。

查看检测结果汇总数据

您可在基线检查页面上方，查看云安全中心根据不同基线检查策略，在您资产中检测到的基线检查结果汇总数据。

- 检查服务器数：云安全中心执行基线检查的服务器数量。

  检查服务器数是您在配置基线检查策略时，勾选的分组服务器中服务器的总台数。
- 检查项：是您在配置基线检查策略时，勾选的基线名称的数量。
- 最近检查通过率：最近一次执行基线检查的基线合格率。

  最近检查通过率字体为绿色时，代表扫描的资产中基线配置合格率较高；字体为红色时，说明检查的资产中不合格的基线配置较多，可能存在安全隐患，建议前往基线检查详情页面查看并修复。

  在基线检查详情页面，单击各资产操作栏下的查看，可查看并尽快加固检查状态是未通过的基线配置。

即时手动基线检查

云安全中心基线检查功能支持周期性自动扫描（配置基线检查策略时，选择检测周期即可定时自动扫描）和即时手动扫描（执行立即检测）。

1. 登录云安全中心控制台。
2. 在左侧导航栏，单击安全防范 > 基线检查。
3. 在基线检查策略下拉框中，选择需要执行即时手动检查的基线策略。

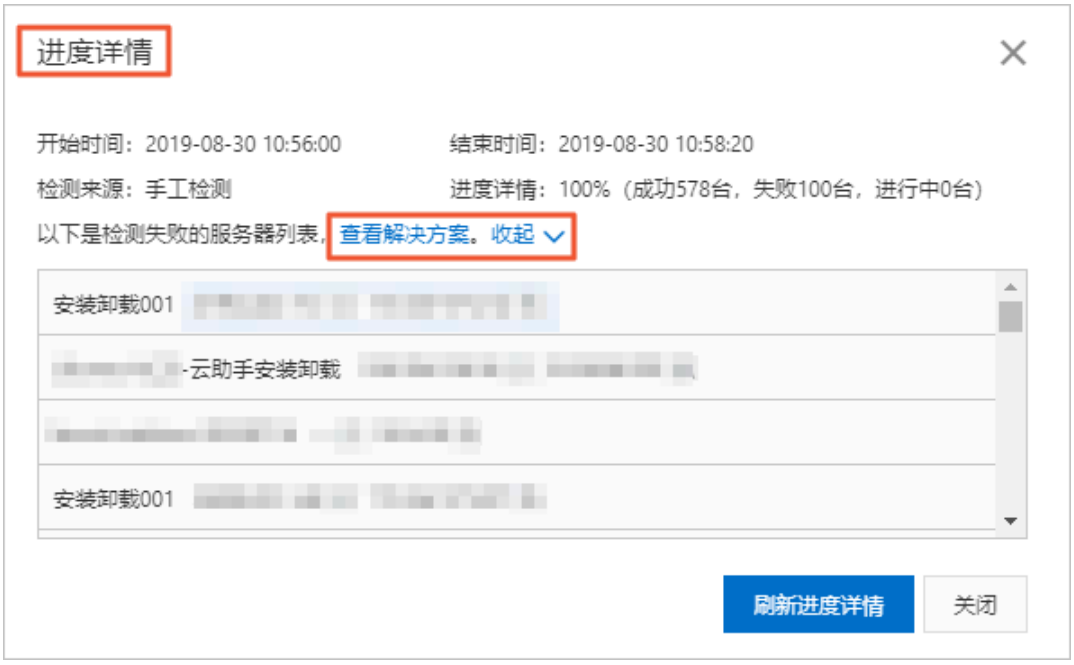
> 说明:

风险项/影响服务器数不为0，表示有服务器未通过该基线检测，服务器存在风险隐患。

4. 单击立即检测。

- 执行立即检测后，检测概览区域将显示实时检测进度。

- 执行立即检测后，单击检测概览区域的进度详情，可展示当前已检测成功/失败的服务器数量以及检测失败的原因。您可单击查看解决方案了解详细的修复方案。



单击刷新进度详情，可查看更新的检测结果。

查看基线检查详情

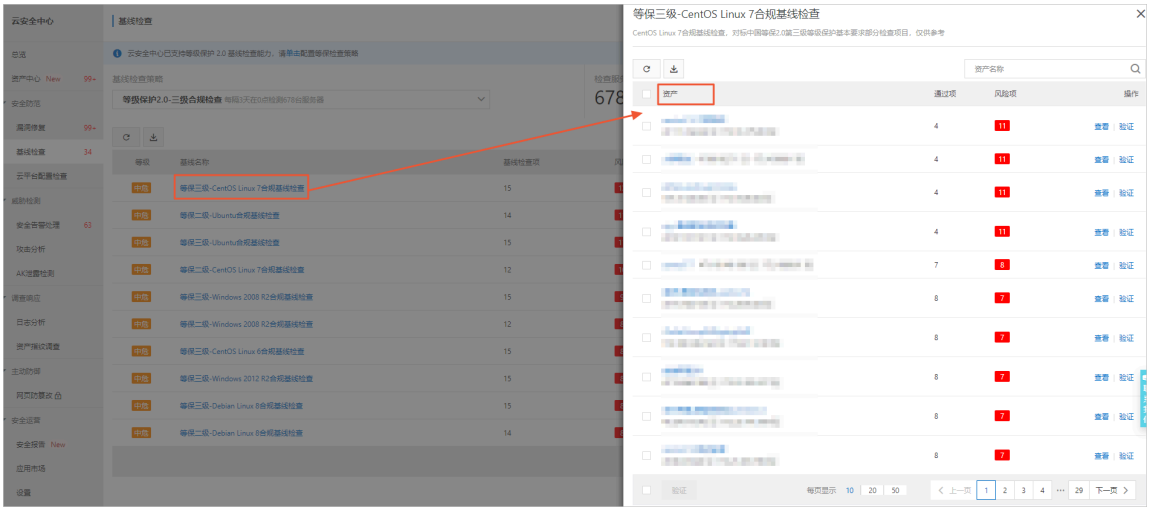
基线策略扫描完成后，您可在基线检查列表中，单击基线名称，打开该基线项目的详情页面。

您可查看该基线项影响的所有资产、风险项合格状态、加固建议等，还可对检测未通过的基线项目执行忽略，或对已完成修复的基线项目执行验证。

1. 登录云安全中心控制台。
2. 在左侧导航栏，单击安全防范 > 基线检查。
3. 在基线检测列表的基线名称栏中，单击待查看的基线项。

4. 您可以根据需要，在基线详情页面执行以下操作。
   - 查看该基线项目影响的所有资产信息。

     您可以对已处理风险项的资产，执行验证。



   - 查看单个资产的详细基线配置风险项信息。

     在详情列表中，单击单个资产右侧操作栏下的查看，可查看单个资产的详细基线配置风险项和风险项的检测结果（已通过/未通过）。

> **说明:**

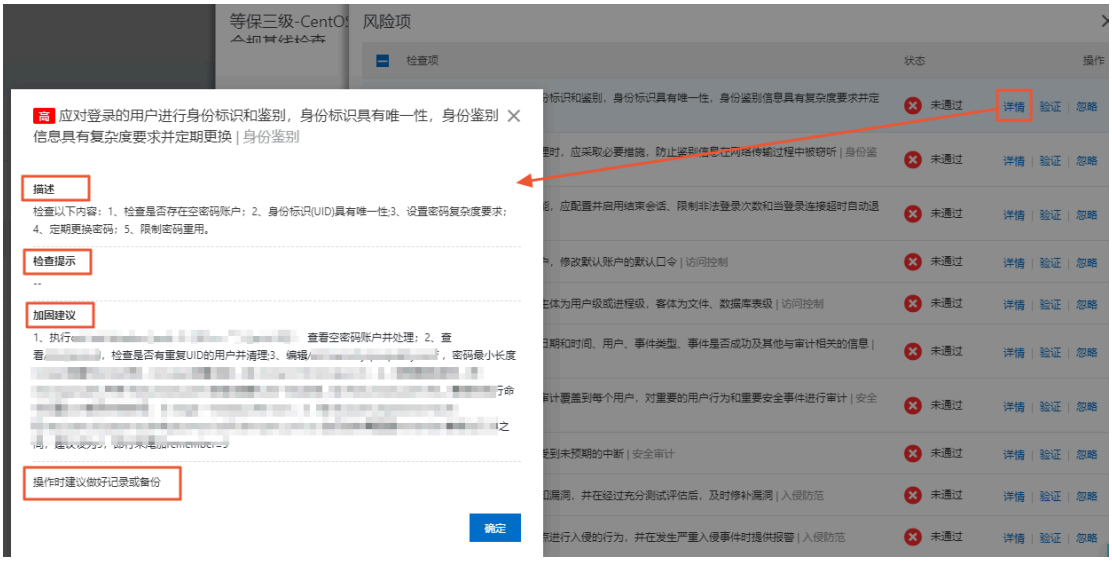
建议对未通过检测的基线项目进行加固，对高危险等级的风险项立即加固。

在风险项列表中，您可以根据需要查看基线检查配置项详情，并处理基线检查配置项。

- **查看基线检查配置项详情**

  单击检查项右侧操作下的详情，查看该风险项的详细描述、提示和加固建议。

  建议根据加固建议对基线配置进行修复或加固。

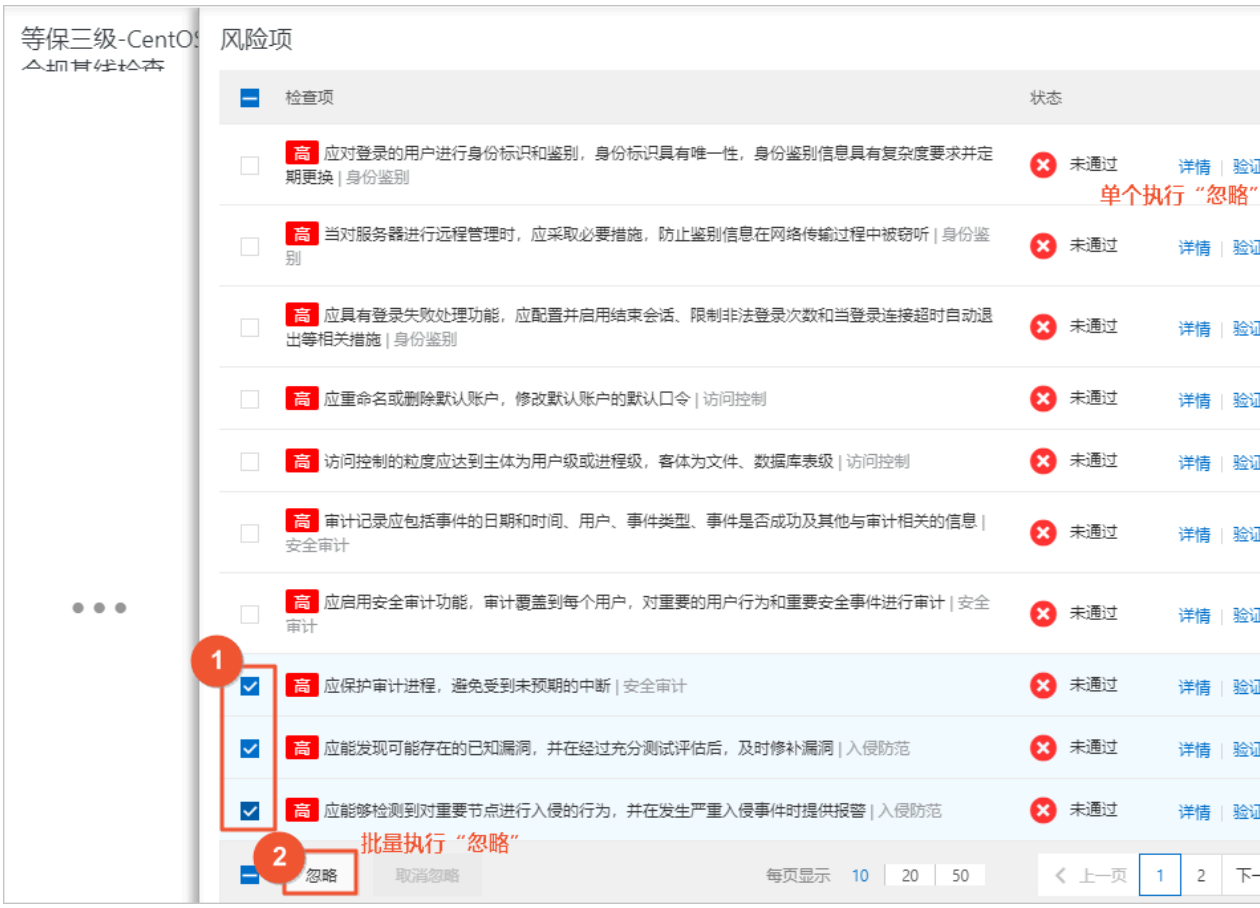


说明:

建议对高危险等级的基线配置项尽快执行加固。

- **忽略指定的基线检查配置项告警**

如果您不希望收到指定的基线检查项的告警，可对指定检查项执行忽略，将检查项告警从基线检查告警列表中移除。支持单个/批量忽略的操作，忽略后，该基线检查项将不再触发告警。



说明:

勾选多个检查项后，单击左下角的忽略，可批量执行忽略操作。

- 取消忽略的基线检查配置项告警

如果需要云安全中心对已忽略的基线检查配置项再次触发告警，您可对忽略的基线检查配置项，执行取消忽略的操作。支持单个/批量取消忽略的操作，取消忽略后，该基线检查项会再次触发告警。

- 验证已加固的基线检查配置项

基线项目加固后，单击验证，一键手动验证该基线项目是否已修复成功。执行验证后，该项目状态将显示为验证中。

如果您未进行手动验证，云安全中心将会根据您在扫描策略中设置的检测周期执行自动验证。

3 云平台配置检查

本文档介绍了云平台配置检查功能可检测的项目和相关操作。

背景信息

云安全中心云平台配置检查从身份认证及权限、网络访问控制、数据安全、日志审计、监控告警、基础安全防护六个维度为您提供云产品安全配置的检测，帮助您及时发现您的云产品配置风险并提供相应的修复方案。

> 说明:
> 云安全中心基础版的云平台配置检查功能不支持检测所有检查项，高级版和企业版支持检测所有检查项。基础版用户需要升级至高级版或企业版，才能使用云平台配置检查的所有检查项服务。

您可以在云安全中心控制台的云平台配置检查页面，查看已启用检查项数。

云平台配置检查项列表

下表罗列了云平台配置检查项，高级版和企业版支持检测所有检查项，基础版存在差异，其中用到的标识：

- X：表示不包含在服务范围中。
- √：表示包含在服务范围中。

支持的检查项	检查类型	说明	基础版	高级版/企业版
云平台-操作审计配置检查	日志审计	检测是否有开启云平台操作审计功能。未开启操作审计，将无法对管理员在云平台的操作行为进行记录、也不符合合规要求。	X	√
ECS-安全组策略	网络访问控制	检测ECS访问策略。建议安全组最小粒度开放访问策略，仅对必须全网开放的服务才开启0.0.0.0/0，例如80、443、22、3389端口。	X	√
OSS-Bucket服务端加密	数据安全	检测OSS Bucket是否开启数据加密功能。OSS提供服务器端加密功能，对持久化在OSS上的数据进行加密保护，建议您对敏感类型数据开启。	X	√

支持的检查项	检查类型	说明	基础版	高级版/企业版
OSS-Bucket防盗链配置	网络访问控制	检测OSS-Bucket是否开启防盗链功能。OSS防盗链功能通过检查Referer，进行白名单限制，可以用于防止他人盗用OSS数据，建议您开启。	X	√
OSS敏感文件泄露	数据安全	检测OSS敏感文件是否有设置访问权限。	X	√
RDS-跨地域备份	数据安全	检测RDS数据实例是否开启跨地域备份功能。RDS为MySQL提供跨地域备份功能，可以自动将本地备份文件复制到另一个地域的OSS上，跨地域的数据备份能够有效的实现异地容灾。建议您开启跨地域备份。	X	√
Redis-备份设置	数据安全	检测Redis数据库实例是否开启了数据备份功能。	X	√
MongoDB-日志审计	日志审计	检测MongoDB数据库是否开启审计日志功能。云数据库MongoDB审计日志记录了您对数据库执行的所有操作。通过审计日志记录，您可以对数据库进行故障分析、行为分析、安全审计等操作，有效帮助您获取数据的执行情况。建议您开启MongoDB数据库审计日志功能。	X	√
MongoDB-SSL开启	数据安全	检测MongoDB数据库是否开启SSl加密。为提高MongoDB数据库数据链路的安全性，建议您启用SSL加密。	X	√
MongoDB-备份设置	数据安全	检测云数据库MongoDB是否开启自动备份功能。数据库定期备份有利于提升数据库安全，在出现数据库异常时可以根据历史备份信息进行恢复。云数据库MongoDB提供了自动备份策略，建议您保持开启，确保每天备份一次。	X	√

支持的检查项	检查类型	说明	基础版	高级版/企业版
云监控-主机插件状态	监控告警	检测ECS主机运行状态。云监控可以针对阿里云资源和互联网应用进行监控，为了监控ECS主机运行状态，并在出现主机异常指标时可以告警通知，建议在ECS主机安装云监控主机插件。	X	√
VPC-DNAT管理端口开放	网络访问控制	检测端口是否映射到公网。建议VPC NAT网关创建DNAT规则时不要将内部管理端口映射在公网，例如所有端口都映射，或者22、3389、1433、3306等重要端口。	X	√
云平台-主账号双因素认证	主账号身份认证及权限	检查是否开启主账号双因素认证配置。在只使用单一密码认证的情况下，黑客可能通过暴力破解等手段获取您的云平台管理密码。建议对云平台管理员账号开启密码加手机短信双重身份认证，防止密码泄露带来的安全隐患。	√	√
RAM-子账号多因素认证	子账号身份认证及权限	检查子账号是否启用了多因素认证（Multi-Factor Authentication，简称MFA）。	√	√
云盾-主机安全防护状态检查	基础安全防护	检测安骑士Agent插件安装情况。云安全防御体系中，需要部署安骑士解决主机安全防护问题。未部署安骑士将导致云主机缺乏入侵检测及防御的能力，系统无法及时发现各种黑客入侵行为，例如：上传的Webshell、木马等恶意文件、异地登录、账号暴力破解攻击等。	√	√
云盾-高防回源配置检查	网络访问控制	检测DDoS高防服务是否有配置仅允许WAF回源IP地址访问。使用DDoS高防服务或Web应用防火墙后，需要对后端服务器真实IP地址进行隐藏，避免攻击者绕过高防或WAF直接攻击云主机。	√	√

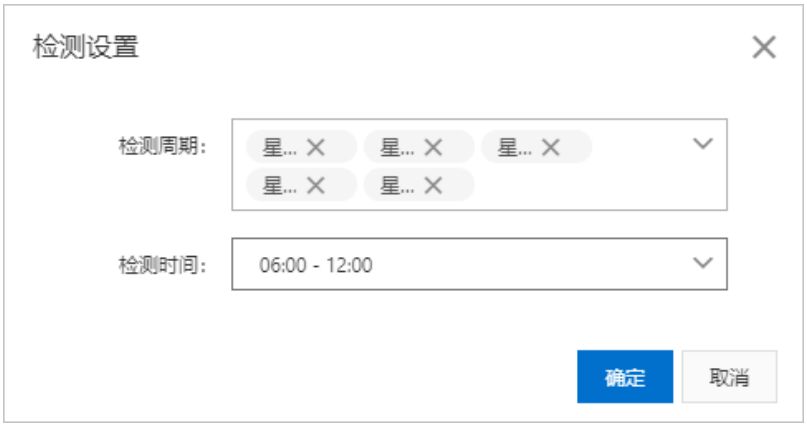
支持的检查项	检查类型	说明	基础版	高级版/企业版
云盾-WAF回源配置	网络访问控制	检测WAF（Web应用防火墙）服务是否配置仅允许WAF回源IP地址访问。使用DDoS高防服务或Web应用防火墙后，需要对后端服务器真实IP地址进行隐藏，避免攻击者绕过高防或WAF直接攻击云主机。	√	√
云盾-AK&账密泄露检测配置	监控告警	检测是否已开启云安全中心AK&账密泄露检测功能。	√	√
ECS-密钥对登录	身份认证及权限	检测ECS中的Linux主机是否绑定了阿里云SSH密钥对。SSH密钥登录与SSH密码登录方式相比，更加安全便捷。推荐使用阿里云SSH密钥对方式。	√	√
ECS-存储加密	数据安全	检测ECS主机磁盘是否开启了加密功能。	√	√
ECS-自动镜像	数据安全	检测ECS磁盘是否开启自动快照功能。自动快照可以提升ECS主机的数据安全，实现容灾备份。	√	√
SLB-白名单配置	网络访问控制	检测SLB负载均衡实例访问控制配置，http/https服务是否启用了访问控制，并且是否有开放0.0.0.0/0。	√	√
SLB-高危端口暴露	网络访问控制	检测SLB是否开转发非必要的公共服务端口。	√	√
SLB-健康状态	监控告警	检测SLB后端服务器是否可用。	√	√
SLB-证书过期检	监控告警	检测SLB的可用证书是否已过期。	√	√
OSS-Bucket权限设置	数据安全	检测OSS Bucket权限是否设置成了私有。	√	√
OSS-日志记录配置	数据安全	检测OSS是否有开启日志记录功能。	√	√
OSS-跨区域复制配置	数据安全	检测OSS是否有开启跨区域复制功能。	√	√
RDS-白名单配置	网络访问控制	检测RDS的访问控制策略是否有0.0.0.0/0（任意IP）或为空的配置。不建议数据库类服务直接对公网开放，需要限定访问范围为指定IP访问。	√	√

支持的检查项	检查类型	说明	基础版	高级版/企业版
RDS-数据库安全策略	数据安全	检测RDS数据库是否开启了SQL审计功能、SSL加密传输功能和透明数据库加密功能。	√	√
RDS-开启数据库备份	数据安全	检测RDS数据库实例是否开启了数据备份功能。	√	√
Redis-白名单配置	网络访问控制	检测Redis的访问控制策略是否有0.0.0.0/0（任意IP）或为空的配置。不建议数据库类服务直接对公网开放，需要限定访问范围为指定IP访问。	√	√
分析型数据库PostgreSQL版-白名单配置	网络访问控制	检测PostgreSQL的访问控制策略是否有0.0.0.0/0（任意IP）或为空的配置。不建议数据库类服务直接对公网开放，需要限定访问范围为指定IP访问。	√	√
SSL证书-有效期检查	数据安全	检测SSL证书是否超出有效期。如果证书过期，您将无法继续使用SSL证书服务。	√	√
POLARDB-白名单配置	网络访问控制	检测云数据库POLARDB的访问控制策略是否开放公网访问且有`0.0.0.0/.0`（任意IP）的配置，不建议数据库类服务直接对公网开放，需要限定访问范围为指定IP访问。	√	√
操作审计-日志配置	日志审计	检测对象存储服务（OSS）或者（日志服务）SLS中的操作日志。 云安全体系要求云平台开启操作审计功能，操作日志需保存在对象存储服务（OSS）或者（日志服务）SLS中，并合理设置日志的访问权限，以实现高危操作可追溯。	√	√
MongoDB-白名单配置	网络访问控制	检测MongoDB的访问控制策略是否有`0.0.0.0/.0`（任意IP）或为空的配置。不建议数据库类服务直接对公网开放，需要限定访问范围为指定IP访问。	√	√

操作步骤

1. 登录云安全中心控制台。
2. 在左侧导航栏，单击安全防范 > 云平台配置检查。
3. 您可在云平台配置检查页面，查看检测结果统计、执行检测或设置检测任务周期。
   - 检测设置
     a. 单击云平台配置检查页面右上角的检测设置，进入检测设置页面。

     b. 设置云产品配置项的检测周期和检测时间。



     检测周期可选周一至周日，支持多选。

     检测时间可选4个时间段中的任一时间段。在选定时间段内，云安全中心会对所有检测项自动执行一次检测。默认每隔1天的`00:00:00-06:00:00`执行自动检测。

     c. 单击确定。
   - 立即检测

     单击云平台配置检查页面右侧的立即检测，对云产品配置进行全量检测，确定是否存在风险项以及影响的资产数量。检测项列表中按检测结果的严重等级由高危到低危进行排序。

> **说明:**

全量检测需全部完成后才可进行其他操作，请耐心等待。

- 验证

  如果您对部分配置项进行了修改，可单击验证检验新的配置是否存在安全风险。

- 忽略

  如果您判断检测出的某个风险项不存在安全风险，可单击忽略将该检测项状态调整为已忽略。已忽略的检测项将不会包含在风险项总数中。

  在检测项列表中，您也可对已忽略的检测项取消忽略。

  
  说明:
  忽略只对本次检测结果进行忽略，后续如果再次检测该出该风险，云安全中心仍会展示该检测结果的告警。

- 查看检测详情

  - 单击基线检测项名称，可跳转到详情页面，查看对应的检测详情描述、可能产生的影响和处理建议。

  - 如果检测到威胁影响中有受影响的资产信息，您可以单击实例ID或实例名，跳转至对应的云产品实例页面，对风险配置项进行配置修改。

- 导出检测结果

  导出检测结果Excel文件到本地。

  
  说明:
  云平台配置检查的检测结果导出功能需为企业版功能，基础版和高级版不支持。基础版和高级版用户需先升级到企业版，才可使用此导出功能。