阿里云 云安全中心(态势感知)

安全防范

文档版本: 20190919

为了无法计算的价值 | 【-】阿里云

<u>法律声明</u>

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。

- 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。
- 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。
A	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。
Ê	用于补充说明、最佳实践、窍门等,不 是用户必须了解的内容。	道 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 listinstanceid Instance_ID
[]或者[a b]	表示可选项,至多选择一个。	ipconfig [-all -t]
	表示必选项,至多选择一个。	<pre>swich {stand slave}</pre>

目录

法律声明	.I
通用约定	.I
1 漏洞修复	1
1.1 漏洞修复必要性说明	.1
1.2 Linux软件漏洞	.3
1.3 Windows系统漏洞1	13
1.4 Web-CMS漏洞 2	<u>23</u>
1.5 应用漏洞	34
1.6 应急漏洞	12
1.7 漏洞管理设置与加白名单4	17
1.8 服务器软件漏洞修复4	18
1.9 漏洞修复优先级排序参考5	50
2 基线检查	3
2.1 基线检查概述5	53
2.2 管理基线检查策略5	54
2.3 执行基线检测5	57
3 云平台配置检查	3

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。
 - ・査看漏洞公告信息

云安全中心	通用体权	系统漂雨扫描时间 : 2019年8月29日 14	438:11 立即扫描 快速修复期间指南 灑洞管理设置
总器	Linux软件識詞 705 Windows系统識词 20 Web-CMS識词 6 应用趣词0 应急識词 4		
资产中心 New 99	C ±	未处理 × 高× 中× 低× × 全	都资产分组 > 排班家属网络称成CVE编号 Q
▼ 安全助范	漏洞公告	影调资产	按照时间 操作
漢河修复 99	□ RHSA-2019:1873-重要: 约岐 security,bug fix,和 enhancement update (调要重量)	221	2019年8月29日 14:16:27 修复
2430位置 34 元平台配置检查	RH54-2019:1880-低急: curl 安全和RUG傳動更新	215	2019年8月29日 14:16:27 修复
■ 1 (1) (1) (1) (1) (1) (1) (1) (1) (1) (RHSA-2019:1884-中德: litesh2 安全興新	218	2019年8月29日 14:16:27 修复

· 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



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。

云安全中心	編開修复 高於集聚白色时间: 2019年3月23日 143811 立即归臣 快速停莫集聚间隔 高兴医学							
.8%		Linux软件期間 705 Windows系统期間 20 Web-CMS期间 6 应用期间						
资产中心 New 99-	-	C ±	未处理 ~	ä× ≠	X 低 X Y	全都资产分组 🗸	请班卖属词名称成CVE编号 Q	
• 安全防范		 憲際公告 			影响资产	披露时间	操作	
漏洞修复 99- 基础检查 34		RHSA-2019:1873-重要:疗纸 security.bug fix,税 enhancement update (電影重命)			221	2019年8月29日 14	16:27 伊賀	
云平台配置检查		RHSA-2019.1880-低微: curl 安全和8UG修复更新			215	2019年8月29日 14	16:27 修复	
7 威胁控测		□ RHSA-2019:1884-中胞-Illosth2 安全更新			218	2019年8月29日 14	16:27 PR	
安全告罄处理 48		RHSA-2017:3263-中位: curl 安全更新			95	2019年8月29日 14	15:10 Pag	
攻击分析		□ RHSA-2018.0666-中僚: krb5 安全和8UG修规更新			122	2019年8月29日 14	:15:10 伊賀	
AK进露检测		□ RHSA-2018.0805.中性: gibt 安全和BUS排版图新 (存在DDP)(代码NG7)			83	2019年8月29日 14	:15:10 (FS	
• 调查响应		RHSA-2018:0849- 临险: gcc 安全和BUG俳复更新			111	2019年8月29日 14	15:10 (F S)	
日志分析		□ RHSA-2018.0855-中性: ntp 安全和BUG橡板更新			136	2019年8月29日 14	15:10 (9.8	
(4)产制的/mity 资产指纹调查		RHSA-2018.1700-重要 procps-ng 安全更新 (存在EXP) (本地提权)			37 97	2019年8月29日 14	:15:10 ØM	
* 主动防御		RHSA-20183059-版他: Xorg X11 安全问题UG博复更新			180	2019年8月29日 14	:15:10 @ M	
用页防要改合		☑ RHSA-20183071-低饱: kb5 安全和8UG修复更新			167	2019年8月29日 14	:15:10 伊賀	
• 安全运营		☑ RHSA-2018.3083.重要:内核安全们BUG修复更新 (票要重用)(存在EXP)(本批Ⅰ度反)			60 123	2019年8月29日 14	:15:10 (PSE	
安全报告 New		☑ RHSA-20183092-中微 glicx 安全和BUG修复更新 (代码执行) (本地提标)			38 86	2019年8月29日 14	:15:10 修复	
安全大屏		RHSA-2019.0201-版地: systemd 安全要新			179	2019年8月29日 14	15:10 修 复	
应用市场		100 max 100 ma		每页显示	R 20 Y	く 上一页 1 2	3 4 … 36 下一页 >	

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。

漏洞管理设置				×
Linux软件漏洞:		共628台 (还有2台未开启	3)	管理
Windows系统漏洞:		共628台 (还有2台未开启	3)	管理
Web-CMS漏洞:		共628台 (还有2台未开启	3)	管理
应急漏洞:		共628台 (还有17台未开	启)	管理
应用漏洞:		扫描周期 ? 一周	\sim	
失效漏洞自动删除:	7天	~		
漏洞扫描等级:	✔ 高	✔ 中 ✔ 低		
漏洞白名单配置:				
✓ 漏洞公告				操作
✔ RHSA-2018:1852-中危	内核安全更新	祈		移除
✔ RHSA-2018:1965-重要	内核 安全和日	BUG修复更新		移除
✔ 移除			く 上一页 1	下一页 >

・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。

云安全中心	編集時度 最終度的目前:2019年4月29日143811 2月1日月1日11 2月1日月1日 2月1日月1日 2月1日月1日		
愁落	Linux软件贏洞 705 Windows系統贏洞 20 Web-CMS亂洞 6 应用贏同0 应急亂詞 4		
资产中心 New 99+	۲ ۲	→ 10月 → 1000 → 1000 → 10000000000	全都资产分组 > 講班家還网名称成CVE编号 Q
▼ 安全助范	調測公告	影响资产	披露时间 操作
進河修复 99+ 36/650-35	RHSA-2019:1873-建築 内核 security.bug fu,和 enhancement update (高安重量)	221	2019年8月29日 14:16:27 修复
云平台配置检查	RHSA-2019:1880-低微: curl 安全和BUG標準更新	215	2019年8月29日 14:16:27 修算
▼ 威胁检测	RHSA-2019:1884-中微: libssh2 安全更新	218	2019年8月29日 14:16:27 伊賀
1	兑明:		

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。

云安全中心	· 通问标复	系統團際扫描时间: 2019年8月29日 1438:11 立刻扫描 快速修复属资捐资
035	Linux软件職間 705 Windows系统應用 20 Web-CMS識問 6 应用識問0 应急識問 4	
资产中心 New	99+ C 🛓	未処理 ∨ 高×中×低×∨ 全部街 [™] 分組 ∨ 排撥要雇用名称成CV(納号)
▼ 安全防范	展网公告	影响资产 按照时间
潤同修复	99- RHSA-2019:1873-重要:内核 security,bug fix,和 enhancement update (宮田東宗)	2019年8月29日 14:16:27
基线检查		
云平台配置检查	RTSA-2019/1000-Itzlg: C01/StdeNoOU398dtsBeft	2013440H29E144(10:27
▼ 威胁检测	RHSA-2019:1884-中版: libssh2 安全更新	218 2019年8月29日 14:16:27

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。
- 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。



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。

^o	
	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。

<u>.</u>

・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
	- 可导致本地拒绝服务的漏洞。
	- 兵他尼古牧瓜的禰何。 ・ 4 0-6 9:中告
	重西进行公五十张影响用白的混调
	- 高安近11父互7
	- 诵讨本地修改配置或获取信息之后,可讲一步利用的漏洞。
	· 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。
	・緊急程度中:
	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。
	 一 命甲: 该漏洞的匹配命甲原因, 一般是田士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。
 - ・査看漏洞信息

云安全中心	波明修 复		系统属洞扫描时间: 201	9年8月29日 14:55:44 立即扫描 は	法修复震荡指南 通河管理设置
83	Linux软件職同 705 Windows系统 期间 20 Web-CMS職间 6 应用職间0 应急職間 4				
资产中心 New 99+	C ±	未处理 ~	高× 中× 低×	◇ 全部街产分組 ◇	请搜索漏洞名称或CVE编号 Q
▼ 安全防范	蕭卿公告		影响资产	扳露时间	操作
新行行 A 34	2019-8-微試安全更新(Windows 2012R2)- K84512469 - 近極處面紛身RDP近極於行代詞期間(CVE-2019-1161/1182)		6	2019年8月29日(08:54:07 伊夏
云平台配置给查	2019-8-微欲安全更新(Windows 2008R2 5P1)- KB4512486 - 运程奠页服务RDP运程执行代码属词(CVE-2019-1181/1182) - 需安装前置补丁K84490628和K84474419		34	2019年8月29日(08:51:13 f#3#

· 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



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。

云安全中心		產用修复	繁統屬開始調明的: 2019年8月	29日 14:55:44 立即扫描 快速修動電荷路南 編詞管理设置
总范		Linux软件编词 705 Windows系统编词 20 Web-CMS编词 6 应用编词0 应急编词 4		
资产中心 New	99+	C 4	★处理 > 高 × 中 × 低 × >	全部资产分组 > 清澄素運河名称或CVE編号 Q
▼ 安全防范		■ 満形公告	影响资产	披露时间 操作
流河修复	99+	2019-8-微軟安全更新(Windows 2012R2)- K84512489 - 過程處面服务RDP過程执行代码購到(CVE-2019-1181/1182)	6	2019年8月29日 08:54:07 修复
基线检查	34	2019-8-微软安全更新(Windows 2008R2 SP1) - KB4512486 - 远程编篇服务RDP远程统行代码稿间(CVE-2019-1181/1182) - 需安装前置补丁KB4490628(IKB447419	34	2019年8月29日 08:51:13 修駕
		2019-7-微软发金更新 (Windows 2012R2) - KB4507457 - 安排补丁可能会导致CPU性能下降	7	2019年8月29日 08:54:07 停旗
 #18/14/20 安全告報分理 	48	2019-7-微软安全更新(Windows 2008R2 SP1) - KB4507456 - 安装补丁可能会导致CPU性能下降	15	2019年8月29日 08:51:13
攻击分析		2019-6-俄欧安全更新 (Windows 2012R2) - K84503290	8	2019年8月29日 08:54:07 修算
AK社靈检測		2019-6-微致安全更新(Windows 2008R2 SP1)- KB4503269	14	2019年8月29日 08:51:13 修复
▼ 调查响应		2019-5-微妙波全奥新(Windows 2012R2)- KB4499165	6	2019年8月29日 08:54:07 修算
日志分析		2019-5-認約安全更新 (Windows 2008R2 SP1) - KB4499175	10	2019年8月29日 08:37:12 修复
微步威胁情报		2019-4-微纹安全亚新(Windows 2012R2)- K84493467	7	2019年8月29日 08:54:07 修練
资产指纹调查		2019-4-微始增全要新 (Windows 2008R2 SP1) - K84493448	16	2019年8月29日 08:51:13 修輝
▼ 主动防御		2014-3-7851年前新聞記録##80565開幕新 (Windows 2008月25日) - K84400538	28	2019年8月29日 08-51-13 伊賀
网页防算改 🖻		2010 2. SERVED-DIREC (Mindows 201102) - VEAL0002		2010/#98208 0954-07
▼ 安全运营 + 4 55 # 1				
安王投告 New 由今十届			20	
应用市场		2019-3-005(WINDOWS SHA-C会会定得受用 (WINDOWS SHO) - 5644/4419	25	2019年8月29日 083 113 193
1.00 (g = 10 mg)				●风豆水 20 ~ 〈 上一页 1 下一页 〉

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。

漏洞管理设置		×
Linux软件漏洞:	共628台 (还有2台未开启)	管理
Windows系统漏洞:	共628台 (还有2台未开启)	管理
Web-CMS漏洞:	共628台 (还有2台未开启)	管理
应急漏洞:	共628台 (还有17台未开启) 管理
应用漏洞:	扫描周期 ? 一周	\sim
失效漏洞自动删除: 7天	~	
漏洞扫描等级: 🗾 🔽 高	✔ 中 ✔ 低	
漏洞白名单配置:		
✓ 漏洞公告		操作
✓ RHSA-2018:1852-中危: 内核 安全更新	祈	移除
✓ RHSA-2018:1965-重要:内核 安全和B	BUG修复更新	移除
✔ 移除		く 上一页 1 下一页 >

・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。



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。
- 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。

云安全中心	調用修業	☆ 2019-7-微软安全更新 (Windows 2012R2) - KB4507457 - 安装补丁可能会导致CPU性能下降 加入日名単 3
88	Linux软件網用 705 Windows系统機關 22 Web-CMS 课间 7 应用 應詞 应急 贏詞 4	
资产中心 New 99+	c ±	简介
▼ 安全防范	· · · · · · · · · · · · · · · · · · ·	CN2-2019-1102 GBI 1运程执行代码题明
潤潤修复 99+	2019-8-微软安全更新(Windows 2012R2)- KB4512469 - 远程卓重服弱乐DP远程执行代码震调(CVE-2019-1181/1182)	Windows器形设备推口(GII)处理的存中对象的方式中存在一个远程执行代码罷得。成功利用此罷解的项击者可以控制预测师的系统。
基线检查 31	2019-8-微软安全更新(Windows 2008R2 SP1) - K84512486 - 远程桌面服务RDP远程执行代码编阅(CVE-2013-1181/1182) - 案	CVR-2019-0765(Visidors 1002種名書近程执行作用編用 当改造者符件物版描述设法到MITT始厚林移稿芬题时,Visidors Server DNIT服务中存在内许用扩展词。成功利用此推测的改造者可能在MITT始厚林移稿芬数上运行任意代码, #TTTTNANGHTMT
云平台配置检查 8	2019-7-微敏快会要新(Windows 2012R2)- KB4507457 - 安納补丁可能会导致CPU性能下降	w-www.rteemery。
 - 成初投刻 - 成初投刻 - 成初行政制 - 成初 	2019-7-微软安全更新(Windows 2008R2 SP1)- K84507456 - 安装补丁可能会导致CPU性能下降	当Windows AppI部署器务(AppZSTC)不正确地处理硬防接时,存在一个特权提升器网。
攻击台管儿法 337	2019-6-微软安全更新(Windows 2012R2)- KB4503280	CV2-C019-0011 Vindows DDS服务器师绝压务推测 Vindows DDS服务器无法正确心理DDS宣称计 存在拒绝服务推测。
AK过露检测	2019-6-微說安全更新(Windows 2008R2 SP1)- K84503269	CVW-0019-0680 Nicrosoft splwweid+特权提升羅問 valweid wa/MWII至WNWEIDADT+14-027人本ftHMD用+1#W目。
▼ 调查响应	2019-5-微欲安全更新 (Windows 2012R2) - K84499165	CTV2-2019-1125 Findows 内核位度思想驚躍(安珠补丁可能会导致CTV性性下评)
日志分析	2019-5-微弦定金運新(Windows 2008R2 SP1)- K84499175	2018 年 1 月 3 日,Microsoft 发布了与一类能发现的硬件赢到(称为 Spestre)根廷的公告和安全更新程序,这些赢得涉及不规程度影响 AMB、AAM. A Intel CPU 的建理执 行边信道。此需用于 2019 年 8 月 6 日波布,它是 Spectre Variant 1 補肥時行边信道應用的资体,已被指定为 CVZ-2019-1125。
微步或防備报	2019-4-微欲定金運新(Windows 2012R2)- KB4493467	
资产指纹调查	2019-4-微软g金更新(Windows 2008R2 SP1)- KB4493448	★ C と 未記環 ∨ 金部体本 × 高 × 中 × 伝 × ∨ 金部団产分組 × 編入服防器回転名称 Q
★ 主动防御	2019-3-微軟更新級务機構的必要更新(Windows 2006R2 SP1)- KB4490628	医急性度 🔮 影响宽声
内贝研表式 益 ▼ 由今活業	2019-3-微软皮全更新(Windows 2012R2)- KB4489683	□
安全报告 New	2019-3-微訪安全更新(Windows 2008R2 SP1)- K84489885	▲ ····································
应用市场	2019-3-微软Windows SHA-2签名支持更新(Windows 2008R2 SP1) - K84474419	
		1 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2

- 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。

2019-7-微软安全	全更新(Windows 2012R2)- KB	4507457 - 安装补丁可能会导致CPU性能下	降 加入白名单 🗙
漏洞详情 待处理	漏洞 8 川山、中小十1主华-地行汉征川和河。		
CVE-2019-1125 Windows 内材 2018 年 1 月 3 日,Microso 行边信道。此漏洞于 2019 年	该信息泄漏漏洞(安装补丁可能会导致CPo性能下 sft 发布了与一类新发现的硬件漏洞(称为 Spe 8 月 6 日发布,它是 Spectre Variant 1 推	7度) >tre)相关的公告和安全更新程序,这些漏洞涉及不同程度影响 里执行边信道漏洞的变体,已被指定为 CVE-2019-1125。	AMD、ARM 和 Intel CPU 的推理执
* C 7	未处理 > 全部状态 >	○高 × ○中 × ○低 × ○ ★ 全部资产分组	・ 輸入服务器IP或名称 Q
✓ 緊急程度 Ø	影响资产	状态	操作
✓ 高	CONTRACTOR OF STREET,	未修复	详情 修复验证
✓		未修复	洋情 修复 验证 😳
	10000000000000000000000000000000000000	未修复	详情 修复 验证 :
<mark>▼ 高</mark>		未修复	详情 修复验证 🚦
✓ 高	hills / House	未修复	洋情 修复验证 🚦
✓ 高	and the second second	未修复	洋情 修复验证 🚦
✓ 高	and a local sector	未修复	洋情 修复 验证 :
✓ 高	CONTRACTOR OF	未修复	详情 修复 验证 :
✓ 修复 登证	忽略	每页显示 10 20 50	く 上一页 1 下一页 >

・ 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。



建议立即修复高危漏洞(紧急程度高)。

・査看漏洞详细状态

- 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。

2019-7-微软安全	ē更新(Windows 2012R2)- K	B4507457 - 安装补丁可能会导致CPU性能	起下降 加入自名单
漏洞详情 待处理》 Spirwowow.exe双理未空调用ing/	漏洞 8 ハエトギリナはキャビは1次症ノリ和利。 2位自世震震洞(安英社下司能会导致cpw性能	下版)	
2018 年 1 月 3 日,Microsof 行边信道。此漏洞于 2019 年	th 发布了与一类新发现的硬件漏洞(称为 Sp 8 月 6 日发布,它是 Spectre Variant 1 拍	(1997) eestre)相关的公告和安全更新程序,这些漏洞涉及不同程度) 倒理执行边信道漏洞的变体,已被指定为 CVE-2019−1125。	影响 AMD、ARM 和 Intel CPU 的推理执
★ C 7	未处理 > 全部状态 >	「高 X 中 X 低 X Y 全部资产分	组 > 輸入服务器IP或名称 Q
✓ 緊急程度 🛿	影响资产	状态	操作
✓	resort Parries.	未修复	洋情 修复 验证 :
✓ 高	1 Mar 1 1 - 1 1 1 1 1 1 1 1 1 1	未修复	详情 修复验证 🗄
✓ 高		未修复	^{这444} 详情 修复 验证 :
☑ 高	CONTRACTOR NO.	未修复	详情 修复验证 :
2 高	Million and	未修复	详情 修复验证 :
高		未修复	详情 修复验证 :
✓ 高	and a local design of the	未修复	详情 修复验证 :
✓ 高	CONTRACTOR OFFICE	未修复	详情 修复验证 :
✓ 修复 验证	忽略	每页显示 10 20 50	く 上一页 1 下一页 >

- 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:

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。・捜索漏洞影响资产

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。

云安全中心		通问体复	☆ 2019-7-微软安全更新 (Windows 2012R2) - KB4507457 - 安装补丁可能会导致CPU性能下降 加入由名单	
#X		Linux软件識词 705 Windows系统應用 22 Web-CMS識詞 7 应用漏洞 应急漏洞 4	藏詞详微 待处理廉詞 8	
语产中心 New		C Ł	能介	
▼ 安全防范		美男公告	CV2-2019-1102 GBI + 远程执行代码最间	
漏洞修复	99+	2019-8-微软安全更新 (Windows 2012R2) - K84512489 - 這程虞国服务RDP這程执行代码應到(CVE-2019-1181/1182)	Windows提取设备接口(GGG)处理内存中对集的方式中存在一个通程执行代码篇词。成功利用此篇项的改击省可以控制规制响的系统。	
基线检查		2019-8-根软支全更新(Windows 2008R2 SP1)- KB4512486 - 近程盧葉跟發RDP近程执行代码編問(CVE-2019-1181/1182) - 電	CDW2019-00% Windows UNT服务型边程取行代码编码 当成由素特特地路接触发送到MUT站内转移服务器时,Windows Server INCT服务中存在内斜闭环器网。成功利用此履用的效击曲可能在UNIT站路转移服务器上运行任意付 或器数WINIT和GNR系。	代词,
大平台配里拉查		2019-7-微软安全更新(Windows 2012R2)- KB4507457 - 安装补丁可能会导致CPU性能下降	CVE-2019-1130 Windows特权提升雇用	
* ABREA		2019-7-微软安全更新(Windows 2008R2 SP1) - K84507456 - 安装补丁可能会导致CPU性能下降	当Windows App2部署指示(App2SWC)不正确地处理硬链接时,存在一个特权提升器间。	
攻击分析		2019-6-微软安全更新(Windows 2012R2)- KB4503290	CVE-2019-0611 Winders DOS服务署巡绝服务署词 Winders DOS服务署天全正确已受DOS宣邮时,存在拒绝服务需词。	
AK世露检测		2019-6-俄款安全更新(Windows 2008R2 SP1)- KB4503269	CYE-2010-0800 Nierssoft splave64特权遵升編問 columnia en.AM専業政治国的内容力力方式大地通知原料解释。	
▼ 调查响应		2019-5-微软安全更新(Windows 2012R2)- KB4499165	CVE-2019-1125 Windows 内核信息泄理罪第 (安装补丁可能会导致CFridt能下降)	
日志分析		2019-5-微软g全提新(Windows 2008R2 SP1)- KB4499175	2018 年 1 月 3 日,Nierzeuft 发布了与一类钢拔划的硬件器用(称为 Spetre)相关的公告和安全更新程序,这些理论技不同程度影响 AMD、ADM 和 Latel CPU 的 行边信道。此器码子 2019 年 8 月 6 日发布,它是 Spetre Variant 1 推理执行边信道器和的变体,已被指定为 CPZ-2019-1125。	推理执
微步威胁情报		2019-4-微软安全更新 (Windows 2012R2) - K84493467		_
资产指纹调查		2019-4-彻软安全更新(Windows 2008R2 SP1) - KB4493448	★ C と 未处理 ◇ 金都秋古 ◇ 高 × 一番 ✓ 金都数件分組 ◇ 輸入服务器印成名名	a Q
▼ 主动防御		2019-3-微欽更新證施模线的必要更新 (Windows 2008R2 SP1) - K84490628	■ 緊急性変 ● 影响性产 状态	操作
同页防装改 品		2019-3-微软g全要新(Windows 2012R2)- KB4489883	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	80Z I (
* 女王忠喜 安全报告 New		2019-3-微软安全类新(Windows 2008R2 SP1)- KB4489885		RE I
应用市场		2019-3-微软Windows SHA-2签名支持更新(Windows 2008R2 SP1) - KB4474419		
-0.00			日 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二	1917 I
-				

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。

2019-7-微软安全	更新(Windows 2012R2)- KB	34507457 - 安装补丁可能会导致	女CPU性能下降	加入白名单
漏洞详情 待处理》	漏洞 <mark>8</mark>			
Windows DNS服务器无法正确处 CVE-2019-0880 Microsoft s splwow64.exe处理某些调用的方 CVE-2019-1125 Windows 内核 2018 年 1 月 3 日,Microsof 行边信道。此漏洞于 2019 年	理DNS查@时,存在拒绝服务漏洞。 plwow64特权提升漏洞 5式中存在本地特权提升漏洞。 信息泄漏漏洞(安装补丁可能会导致CPw性能T t 发布了与一类新发现的硬件漏洞(称为 Spe 8 月 6 日发布,它是 Spectre Variant 1 推	∑降) ∘tr«)相关的公告和安全更新程序,这些漏洞 理执行边信道漏洞的变体,已被指定为 CVE-20	步及不同程度影响 AMD、ARM 和 I)19-1125。	ntel CPU 的推理执

·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。



- · 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。

・査看漏洞信息

云安全中心	展用体复	系统漏洞扫描时间: 2019	年8月29日 11:24:21 立即扫描 快速修复震调描着	漏洞管理设置
835	Linux软件编词 705 Windows系统编词 20 Web-CMS编词 7 应用编词 0 应参编词 4			
资产中心 New 994	C T	★处理	◇ 全部資产分組 ◇ 清澄支漏洞谷(NSTOCKENNE Q
▼ 安全防范	展開公告	影调资产	披露时间	操作
周河修复 99+	dederms注入尾闭	2	2019年8月29日 09:14:25	修复
型版位型 24 天平台記書校書	dedecms注入规闭	2	2019年8月29日 08:57:03	伊奴
▼ 威胁检测	discust名與你行觸問	1	2019年8月29日 09:49:15	侍复
安全告誓处理 42	echopl主入服用		2019年8月29日 09:49:12	修复
攻击分析	dedecms_L(%)%)	1	2019年8月29日 08:57:08	伊复
AK过露检测	dedecms(主入)规闭	1	2019年8月29日 08:56:53	修复
▼ 调查响应	dedecms(主入)规闭	1	2019年8月29日 08:56:48	修复
日志分析	加入出名单		毎页显示 20 ~ く 上一页 1	下页 >

· 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。

云安全中心	編明修复	系統罵詞扫描时间: 201	9年8月29日 11:24:21 立即扫描 快速修复蒸汽指路 國際管理设置
总资	Linux软件漏间 705 Windows系统漏洞 20 Web-CMS赢闹 7 应用漏洞 0 应急漏间 4		
资产中心 New 99+	с т	★处理	✓ 全部統产分組 ✓ 清強支援同名称或CVE編号 Q
▼ 安全防范	調用公告	影响资产	按整时间 操作
通河修复 99+ III(21)+开 24	dedecms注入通用	2	2019年8月29日 09:14:25 修算
云平台配置检查	dedecms注入通用	2	2019年8月29日 08:57:03 修算
▼ 威胁检测	discut代码执行编网		2019年8月29日 09:49:15 修复
安全告誓处理 42	echopl±A.RR	•	2019年8月29日 09:49:12 修复
攻击分析	dedecms上传篇网	•	2019年8月29日 08:57:08 伊賀
AK建露检测	dedecms注入课程	•	2019年8月29日 08:56:53 伊賀
▼ 调查响应	_ dedecms注入课则		2019年8月29日 08:56:48 修复
日志分析	加入的名称		毎页显示 20 💙 🖌 上一页 1 下一页 >
and Annually			
1	兑明:		

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。

云安全中心		龍狗体変			系统應利扫描时间: 2019年	8月29日 11:24:21 立即扫描:	快速修复漏洞描南	漏洞管理设置
后茂		Linus饮件编词 705 Windows系统编词 20 Web-CMS编问 7 应用编问 应参编词 4						
资产中心 New	99+	с т	未处理	~	高×中×低×	◇ 全部资产分组 ◇	请搜索派词名称	stocve编号 Q
▼ 安全防范		■ 満野公告			影响资产	披露时间		操作
混河停复 第1号10章	99+	dedecmi注入震网			2	2019年8月29日	09:14:25	修展
安平台配置检查	34	dedecms注入漏洞			2	2019年8月29日	08:57:03	伊朗
▼ 威胁检测		discut代码NF展网			1	2019年8月29日	09:49:15	修复
安全告誓处理	42	ecshop(注入通用			1	2019年8月29日	09:49:12	修复
攻击分析		dedecmz上控编网			1	2019年8月29日	08:57:08	修契
AK泄露检测		dedecmi注入漏网			1	2019年8月29日	08:56:53	修展
▼ 调查响应		dedecms注入编网			1	2019年8月29日	08:56:48	傳統
日志分析		■ 2022年8年				每页显示 20 🗸	く 上一页 1	下—页 >

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。

漏洞管理设置		×
Linux软件漏洞:	共628台 (还有2台未开启)	管理
Windows系统漏洞:	共628台 (还有2台未开启)	管理
Web-CMS漏洞:	共628台 (还有2台未开启)	管理
应急漏洞:	共628台 (还有17台未开启)	管理
应用漏洞:	扫描周期 ⑦	
失效漏洞自动删除: 7天	\sim	
漏洞扫描等级: 🔽 高	✔ 中 ✔ 低	
漏洞白名单配置:		
—— 漏洞公告		操作
✓ dedecms注入漏洞		移除
RHSA-2018:1852-中危: 内核 安全更	祈	移除
RHSA-2018:1965-重要: 内核 安全和6	3UG修复更新	移除
移除	<	上一页 1 下一页 >

・捜索漏洞

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。

云安全中心	應用修复	系统属同扫描时间: 2019年8	月29日 11:24:21 立即扫描 快速修复黑洞探南 漂河管理设置
82	Linux软件编词 705 Windows系统编网 20 Web-CMS最同 7 应用编码 应急编码 4		
资产中心 New 99+	C ±	★处理	✓ 全部资产分组 ✓ 请搜索漏洞名称或CVE编号 Q
▼ 安全防范	調査の公告	影响资产	披露时间 操作
第四修复 99+ 第5%音 34	dedecma(注入通知	2	2019年8月29日 09:14:25 修复
云平台配置检查	dedecm:(注入原列	2	2019年8月29日 08:57:03 修复
▼ 威胁检测	discatt词执行篇词	•	2019年8月29日 09:49:15 修覽
安全告替处理 42	esshop注入尾列	•	2019年8月29日 09:49:12 修練
攻击分析	dedecms上按属闭		2019年8月29日 08:57:08 修复
AK过露检测	dedecms注入漏闭		2019年8月29日 08:56:53 停駕
▼ 调查明应	dedecms注入课程	•	2019年8月29日 08:56:48 修算
出た方町	 加入出名单。 	ŧ	頑显示 20 💙 🖌 上一页 1 下一页 >

道 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。

云安全中心		通用修复			系统	电局间扫描	副町田: 2019	₩8月29日	11:24:21 立即扫描(夫违律复震洞探南	混消管理设置
总路		Linux软件编词 705 Windows系统编词 20 Web-CMS编词 7 应用编词0 应意编词 4									
资产中心 New	99+	C 4	未处理	~	裔 ×	Ф X	任 ×	~	全部资产分组 🗸	请按索漏洞名和	INSTOCUEIRAN Q
▼ 安全防范		蕭兩公告					影响资产		披露时间		操作
漏洞修复	99+	dedecms注入源网					2		2019年8月29日	09:14:25	伊夏
基线检查	34	dedecms注入原则					2		2019年8月29日	08:57:03	修算
▼ 威胁检测		discut行码/方案同					1		2019年8月29日	09:49:15	1938
安全告督处理	42	echop进入漏洞					1		2019年8月29日	09:49:12	伊麗
攻击分析		dedecms上按属例					1		2019年8月29日	08:57:08	修复
AK世靈检測		dedecms注入阐词					1		2019年8月29日	08:56:53	修复
▼ 调查响应		dedecms注入 编例					1		2019年8月29日	08:56:48	伊奴
日志分析		加入出名単						每页显示	₹ 20 ¥	< 上一页 1	下一页 >

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。
- 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。

云安全中心	識別修复	🖧 dedecms注入漏洞				
		識問洋脣 待处理識問 4				
88	Linux软件漏洞 705 Windows系统漏洞 20 Web-CMS漏洞 6 应用漏洞0 应急漏洞 4					
资产中心 New 99+	C &	漏洞公告	简介	停复方案		
▼ 安全防范				方案一:使用云盾自研补丁进行一幢修复;		
漏洞修复 99+				方案二:更新读软件到售方局新版本或寻求读软 件提供有的解助。 [注意:读补丁为云盾目研代研修规方案],云盾 会哪哪些当时和马恩不动中于哪自开的体育模式		
基线检查 34	dedecmsi注入编词	dedecms注入漏洞	dedecmo的交量覆盖握何导致注入蓝网。			
云平台配置检查	dedecms注入漏洞	DEDECTIFICATION CONTRACTION OF A CONTRACTION OF A CONTRACTION OF A CONTRACT		一日の日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日本		
▼ 威胁检测	□ discut代码执行篇詞			夏、1934年1月1日(1937年2月24)、可能去等30年 虽然已经使复了该漏洞,云盾依然报告存在漏 洞,遇到该情况可选择忽略该漏洞揭示]		
安全管督处理 48	ecshop注入漏洞					
攻击分析	□ dedecmi_作课词	* ~ *	未处理 × 全部状态 × 高 × 中 × 低 × ×	全部资产分组 > 输入服务器PREA容 Q		
AK世際检測	☐ dedecms注入题词	Sailt 0	影明资产 状态	操作		
▼ 調査明应			统 逾利作 未修复	洋情 停氣 验证 :		
資产損炊调査			*#2	洋橋 修复 验证 :		
▼ 主动防御						
阿贝防蒙政合		 	未修算	洋橋 修駕 验证 🗄		
▼ 安全运营			***	洋情 修复 验证 :		
安全报告 New		● 修复 验证	(2) 部	20 50 く上一页 1 下一页 >		

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。

漏洞详情 待处理漏洞] 4				
漏洞公告	简介		修复方案		
dedecms注入漏洞	dedeoms的变量覆盖漏洞导致注入漏洞。	方案一:使用云盾自 方案二:更新该软件 件提供商的帮助。 【注意:该补丁为云 会根据您当前代码是 进行检测,如果您自 复、或者使用了其他 虽然已经修复了该漏 洞,遇到该情况可选		19目研补丁进行一键修复; 次件到官方最新版本或寻求该 如云盾自研代码修复方案,云 明是否符合云盾自研的修复模 8月行采取了虎层/框架统一作 氧他的修复方案,可能会导致 约漏洞,云盾依然报告存在漏 河选择忽略该漏洞提示]	
¥ C 7	未处理 Y 全部状态 Y 高 X 中 X	(低×) ×	全部资产分组 💙 輸入服务器	P或名称	
- 紧急程度 ?	影响资产	状态		ł	
	镜像制作 	未修复	详情	修复 验证	
☐ <mark>ह</mark>		未修复	详情	修复 验证	
✓		未修复	详情	修复 验证	
☑ 高		未修复	详情	修复 验证	
■ 修复 验证	忽略	每页显示 10 20	50 く 上一页 1	下一页)	

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。

云安全中心	観察制作	返回资产列表			
总派	基本信息 漏洞信息 13 安全告誓处理	基线检查 4 资产指纹调查 44			
资产中心 New 99-	Linux软件漏洞 3 Web-CMS漏洞 10 应用漏洞	应物编词			
▼ 安全防范	* C ±			未处理 ◇ 全部状态 ◇ 高 × 中 × 低 × ◇ dedecms	注入漏洞 (
通用修复 99+	Raug 🛛	披露时间	藏詞公告	状态	担任
基线检查 34		2019年8月28日	dedecms注入漏洞	未修复	洋橋 伊友 絵道 『
云平台配置检查		2019年8月28日	dedecms上传漏洞	未修复	洋橋 伊賀 絵道
* <u>REENEDE</u>		2019年8月28日	dedecms注入腾河	未修复	洋橋 伊賀 絵道
x 主日 新江地 40 攻击分析		2019年8月28日	dedecms注入腾河	未修复	洋橋 伊賀 脸证
AK注握检测		2019年8月28日	dedecms注入漏洞	未修复	洋橋 伊賀 验证

· 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。

🖧 dedecms注入漏洞				加入白名单
漏洞详情 待处理漏洞	3 4			
漏洞公告	简介		修复方案	
dedecms注入漏洞	dedeoms的变重覆盖漏洞导致注入漏洞	lo	方案一:使用云盾目 方案二:更新该软件 件提供商的帮助。 【注意:该补丁为2 会根据您当前代码题 进行检测,如果您目 复、或者使用了其他 虽然已经修复了该派 洞,遇到该情况可说	目研补丁进行一键修复; 牛到官方最新版本或寻求该软 云盾自研代码修复方案, 云盾 星否符合云盾自研的修复模式 目行采取了底层/框架统一修 也的修复方案, 可能会导致您 罵洞, 云盾依然报告存在漏 选择忽略该漏洞提示]
★ C 7	未处理 🗸 全部状态	✓ 高 × 中 × 低 × ✓	全部资产分组 💙	輸入服务器IP或名称 (
緊急程度		状态		提
	1922 漏洞已经过工程师确认可导致严重危 1修复	未修复		详情 修复 验证
「解注如具法	: 请堂着 現像制作	未修复		详情 修复 验证
门 说明:				

-

Web-CMS类型漏洞建议尽快修复。

・捜索漏洞

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。

🛱 dedecms注入漏洞				加入白名单
漏洞详情 待处理漏洞	₱ 4			
漏洞公告	简介		修复方案	
dedecms注入漏洞	dedeoms的变重覆盖漏洞导致注入漏洞。		方案一:使用云盾 方案二:更新该软 件提供商的帮助。 【注意:该补丁为; 会根据您当前代码; 进行检测,如果您 复、或者使用了其; 虽然已经修复了该 洞,遇到该情况可;	自研补丁进行一键修复; 4到官方最新版本或寻求该; 云盾自研代码修复方案, 云/ 是否符合云盾自研的修复模; 自行采取了底层/框架统一修 也的修复方案, 可能会导致; 漏洞, 云盾依然报告存在漏 选择忽略该漏洞提示】
★ C 7	未处理 V 全部状态 V 高 X 中	× 低× ×	全部资产分组 💙	输入服务器IP或名称
紧急程度 🖉	影响资产	状态		扬
	······································	未修复		详情 修复 验证
		未修复		详情 修复 验证
हे बि	And the second second	未修复		详情 修复 验证
<u>व</u>	A DOLLAR DOLLARS	未修复		详情 修复 验证
〕 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。

🖧 dedecms注入漏洞				加入白名单
漏洞详情 待处理漏洞	9 4			
漏洞公告	简介		修复方案	
dedecms注入漏洞	dedeoms的变里覆盖漏洞导致注入漏洞。		方案一:使用云盾目 方案二:更新该软件 件提供商的帮助。 【注意:该补丁为2 会根据您当前代码题 进行检测,如果您目 复、或者使用了其件 虽然已经修复了该派 洞,遇到该情况可说	目研补丁进行一键修复; +到官方最新版本或寻求该 员盾自研代码修复方案,云 冒否符合云盾自研的修复模 目行采取了底层/框架统一 也的修复方案,可能会导致 漏洞,云盾依然报告存在漏 选择忽略该漏洞提示]
★ C ₹	未处理 > 全部状态 >	高 X 中 X 低 X Y	全部资产分组 💙	输入服务器IP或名称
✓ 紧急程度 2	影响资产	状态		ł
☑ 高	培逸制作 	未修复		详情 修复 验证
▶ 高		未修复		详情 修复 验证
☑ 高	AND DESCRIPTION OF A DE	未修复		心略 详情 修复 验证
✓ 高		未修复		详情 修复 验证
✓ 修复 验证	忽略	每页显示 10 2	0 50 <	上一页 1 下一页 2

- 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。

蕢 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。

🛱 dedecms注入漏洞			加入白名单
漏洞详情 待处理漏洞	4		
漏洞公告	简介		修复方案
dedecms注入漏洞	dedeoms的变里覆盖漏洞导致注入漏洞。		方案一:使用云盾自研补丁进行一键修复; 方案二:更新该软件到官方最新版本或寻求该载 件提供商的帮助。 【注意:该补丁为云盾自研代码修复方案,云履 会根据您当前代码是否符合云盾自研的修复模式 进行检测,如果您自行采取了底层/框架统一修 复、或者使用了其他的修复方案,可能会导致您 虽然已经修复了该漏洞,云盾依然报告存在漏 洞,遇到该情况可选择忽略该漏洞提示】
* C 7	未处理 ~ 全部状态 ~	高 X 中 X 低 X Y	全部资产分组 💙 输入服务器IP或名称
□ 紧急程度 ❷	影响资产	状态	10
高	竟像制作	未修复	详情 修复 验证

・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。

★ C 7	未处理	~	全部状态	~	高 X	中 ×	低 ×	~	全部资产分组	~	输入服务器IP或名称
保存以下筛选出的所有漏洞为一个漏洞 批次,后续可进行筛选便干持续跟进此	多复 比漏						状态				擅
洞修复情况	ž 1		私				未修复				详情 修复 验证

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。

T

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。

 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。

云安全中心	漏洞修复				系统漏洞扫描时间: 20	19年9月2日 11:08:48 立刻扫描 快速修复漏洞描稿 講問管理设置
总派	Linux软件漏洞 461	Windows系统漏洞 41 Web-CMS漏洞	应用漏洞2 应急漏洞 4			
资产中心 New	96	出口则2久寝闲 秋虚				
▼ 安全防范		74-00-2008/39094				
混涡修复	99+ C Ł			未处理 > 全部状态 >	(高 ×) 中 ×) 低 ×) ∨	请搜索漏洞名称或CVE编号 Q 输入服务器IP或名称 Q
基线检查	29 修复紧急度	漏洞名称	影响资产	披露时间	状态	操作
云平台配置检查	18	WordPress xmlrpc.php 存在SSRF漏洞	The second se	2019年8月29日 02	2:15:04 未修复	验证 忽略 加白名单
▼ 威胁检测 安全告鉴处理	99+	SSH@E□�	100-00 D 00-00-0	2019年9月1日 02:	15:46 未修复	验证 勿略 加白名单
攻击分析		SSH關口令		2019年9月1日 02:	:15:46 未接篇	验证 爆略 加白名单
▼ 過音速応	102 58	取派忽略 加合名单				毎页显示 20 💙 🖌 上一页 1 下一页 🖒

· 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。

云安全中心		漏洞修复								系统】	観河扫描时间: 20	19年9月2日 11:08:48 立即扫描	快速使复震调描	高河管理	R
82		Linux软件漏洞 461	Windows系统漏洞 41 Web-CMS漏洞	应用漏洞2	应急漏洞 4										
资产中心 New	96	● 当前有应用漏洞2个。	共识别3条漏涡数据。												
 ▼ 安全防范 通過修算 	99+	G F				未处理	~	全部状态 🗸	商 X	Ф X	í X Y	请搜索運同名称或CVE编号	Q silves	务器IP或名称	Q
基线检查	29	停复紧急度	震病名称		影响资产			披露时间			状态				攝作
云平台配置检查	18	8	WordPress xmlrpc.php 存在SSRF漏洞					2019年8月29日	E 02:15:04		未修复		1	eje som toe	日名单
▼ 威胁检测 安全告替处理	99+	商	SSHBR⊡�					2019年9月1日	02:15:46		未修复			NE 1944 INF	日名单
攻击分析		ä	SSH砚口令					2019年9月1日	02:15:46		未修复		1	ever norma the	白名单
AK泄露检测 ▼ 调查响应		- 1915 - 2145	8 取消的10年 20日名单									毎页显示 20 ~	< 上一页	1 下一页	>

・査看漏洞详情

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。

云安全中心	週月修复	■ SSH砌口令 × 单击漏涡名俗。打开漏洞详情页面
SK.	Linux软件識詞 461 Windows系统識詞 41 Web-CMS識詞 应用諷詞2 点	SSH朝口令清河:Linux美统口令的长度大把或者复杂度不够,仅包含效学,或仅包含学母等。 意識問 4
资产中心 New 96	O 当你有应用重要2个,共识和3条要求数据。	影响资产
安全防范		應問证明 适成的影响 安全建议 技术参考
運用修复 99+	C 2	
基线检查 29	修复系数度 荒洞名称	
云平台配置检查 18	WordPress xm/rpc.php 7#7ESSRF	35777 (C39843) IRAN 2410 IRAN 2500 WEST 25070 (PANELO)
或建立		
安全告答处理 99+	SSHBRU\$	ACCOUNT FOUND: [ssh] Host: - User: Password: u 3 [SUCCESS]
攻击分析	□	No. And State of Concession of
AK世露检测		造成的影响
调查响应		利用與口令直接登录系统,获取服务器权限、读取甚至修改网站代码。
日志分析		
微步威胁情报		安全建议 你改一会 描加一会复杂意 如何会主小学家母 教家和特殊家产等。
资产描纹调查		
主动防御		技术条制
网页防装改		http://heipaliyun.com
安全运营		
安全报告 New		
应用市场		
设置		50 X62#

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。

高 SSH弱口令
SSH弱口令漏洞:Linux系统口令的长度太短或者复杂度不够,仅包含数字,或仅包含字母等。
影响资产
漏洞证明 造成的影响 安全建议 技术参考
漏洞证明 SSH存在弱密码,成功检测出目标服务器的系统用户名和密码 IP: 端口: 端口: 证明结果信息: ACCOUNT FOUND: [ssh] Host: User: Password: ③ [SUCCESS]
造成的影响 利用弱口令直接登录系统,获取服务器权限、读取甚至修改网站代码。
安全建议 修改口令,增加口令复杂度,如包含大小写字母、数字和特殊字符等。
技术参考 https://help.aliyun.co
验证 忽略 加白名单
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。

漏洞修复			系的	电漏洞扫描时间: 201	19年9月2日 15:10.03 立即扫描 快速修复建调描南	漏洞管理设置
Linux软件漏洞 461	Windows系统漏洞 41 Web-CMS漏洞	应用漏洞2 应急漏洞 4				
● 当前有应用漏洞2个, ;	共识别3条漏洞数据。					
G Ŧ			未処理 × 全部状态 × 高 × 中 ×	低× ×	请搜索漏洞名称或CVE编号 Q 输入服务器	IP或名称 Q
● 修复聚急度	漏洞名称	影响资产	披露时间	状态		操作
	WordPress xmlrpc.php 存在SSRF漏洞	AND AN A REAL PROPERTY OF	2019年9月2日 13:45:55	未修复	验证单个漏洞是否修复成功	忽略 加白名单
	SSH器口令	And And The State of the State	2019年9月1日 02:15:46	未停复	酸罐	忽略 加白名单
	SSH第口令 洞县本修复成功	And and a second se	2019年9月1日 02:15:46	未修复	酸证	忽略 加白名单
	取消忽略 加自名单				毎页显示 20 ~ く 上一页 1	下页 >

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

说明:

■ 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。

漏洞修复					系统漏洞扫描时间: 2019年9月2日 15:10:1	33 立即扫描 快速修复漏洞描南
Linux软件漏洞 461	Windows系统漏洞 41 Web-CMS漏洞 应	用漏洞2 应急漏洞 4				
() 当前有应用漏洞2个,共	1980後還河数据。					
с т			未处理	全部状态 べ 高 X	中 × 低 × × 请搜索漏洞名和	RISCICVE編号 Q 編入服券器IPI認名称 Q
- 修复系命度	漏洞名称	影明进产		披露时间	状态	搵作
	WordPress xmlrpc.php 存在SSRF遭测			2019年9月2日 13:45:55	未修置	单个忽略漏洞 發证 ^{忽略} 加白名单
	SSH₩□Φ	Carlos and Constants		2019年9月1日 02:15:46	未修复	验证 忽略 加白石单
	SSH费口令	Contraction of Contraction		2019年9月1日 02:15:46	未修复	验证 忽略 加白石单
- 1012 (2 1)	₩消息時間 ₩消息時間 加白名単				每页显示 20	✓ く上−页 1 下−页 >

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。

漏洞修复				系统漏洞扫描时间: 2019年9月2日 15:1	0.03 立即扫描 快速修复漏洞指南 蕭將管理设置
Linux软件漏洞 461	Windows系统漏洞 41 Web-CMS漏洞	应用漏洞2 应急漏洞 4			
 当前有应用漏洞2个。 	共识别张属调数据。				
G 7			未処理 > 全部状态 > 高 > (高 >)	中 X 低 X Y 请搜索属同	S称或CVE編号 Q 編入服务器IP或名称 Q
- 修复紧急度	漏洞名称	影响进产	披露时间	状态	搵作
	WordPress xmlrpc.php 存在SSRF震调	1000 C 10 C 10	2019年9月2日 13:45:55	未修复	单个漏洞加白名单 發证 忽略 加白名单
	SSH朝口令	And And T	2019年9月1日 02:15:46	未修复	验证 忽略 加白客单
	55H赛口令 批局多个漏洞加白名单	And the second s	2019年9月1日 02:15:46	未修复	验证 忽略 加曲客单
- 121E (201	8 取消忽略 加白名单			每页显示	20 🗙 🖌 上一页 1 下一页 🖒

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。



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。



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。

 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。

云安全中心	漏闷修复	系统雇用	3篇时间: 2019年8月29日 15:08:18 立即扫描 快速	修复漏洞指南 漏洞管理设置		
82	Linux软件贏同 705 Windows系統贏用 20 Web-CMS贏同 6 应用贏同					
资产中心 New 99+	C		全部 ~	查询漏洞名称 Q		
▼ 安全助范	置用名称	地關約6月1	影响资产数	操作		
周河修复 99+	Webmin這提命令执行篇順(CVE-2019-15107)	2019年8月19日 23:07:50	已检测,智无风险	立即检测		
基地位置 34 云平台配置检查	Apache Solr 這程命令执行諷諷(CVE-2019-0193)	2019年8月6日 20:00:11	已检测,智无风险	立即检测		
▼ 威胁拉测	XStream < 14.11 远程代码执行继续编码	2019年7月29日 11:15:14		立即检测		
安全告替处理 48	Jackson 最新资序列化量用(CVE-2019-14361和CVE-2019-14439)	2019年7月23日 18:19:13	4	立即检测		
攻击分析	farsjion < 1.2.51 运程代码均行推测	2019年7月10日 17:29:39	已检测,智无风险	立即绘制		
AK泄露检测	Redis 4x/5x 远程命令执行能性漏洞	2019年7月9日 19:16:24	已检测,譬无风险	立即检测		
 > 調査明应 日末分析 	10运04 运程代码执行0ds/兼用	2019年6月26日 18:10:48	已检测,看无风险	立即检测		
微步成防情报	Coremai衛置信息治療day溝洞	2019年6月17日 16:51:20	已检测,智无风险	立即绘测		
资产指纹调查	Oracle WebLogic 远程命令执行Oday編网	2019年4月18日 19:30:09 日检测, 智无风险		立即检测		
▼ 主动防御	Spring Cloud Config 极弱远程任意文件 读 印刷同(CVE-2019-3799)	2019年4月17日 14:34:08	已检测,看无风险	立即检测		
阿页防装改 台	Confluence 遗程命令执行策稳满预(CVE-2019-3396)	2019年4月10日 23:29:55	已检测,著无风险	立即绘制		
▼ 安全运营	MongoD8未授权第日令访问属调	2019年3月24日 10:23:35	2	立即检测		
安全报告 New	Spring Boot Actuator 未接权访问远程代码执行篇词	2019年2月28日 19:12:47	已检测,智无风险	立即检测		

・检测漏洞

说明:

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。

云安全中心	運用修築	应急深刻 5个月前 1	MongoDB未授权弱口令访问》	雨洞		
833	Linux软件獲得 705 Windows系統通用 20 Web-CMS週间 6 应用獲得0 应急運用 4	MongoD8数据库未接权 漏洞洋情: https://hel	鹅口令访问第词,漫词危害严重,可以导致 Ip.aiyun.com	数据库数据准置或根制除勤素,从而造成 单击链接,查看漏洞更多(如于重的生产事故。 言思。	
资产中心 New 99+	C	CVE	π	技業时间	2019年3月24日 09:00:54	
安全防范	調査会会	CVSS	π	危险等级	* #	
潤河修复 99+	Webmin资程会会地行業型(VF-2014-15107)	编词特征	9602WE			
基线检查 34		详情				
云平台配置检查	Apache Son Xetewersen (1981)	漏洞地書				
187全第	XStream < 1.4.11 近極代码如何進進業用	开启MongoD8服务后, 助作) ,而且可以远程。	如不添加任何参数,默认是没有权限验证的 方问数据库。	1. 登景的用户可以通过默认端口无需客码	9.対数据库进行任意操作(包	括増、倒、改、豊な
安全告答处理 49	Jackson 最新50年列化蔬用(CVE-2019-14361和CVE-2019-14439)	濃汽成因				
攻击分析	farijion < 1.2.51 远程代码执行篇词	安装完MongoDB服务后 MongoDB启动时添加了	默认有一个admin数强率,此时admin数据t —auth参数,如果没有在admin数据库中添;	率是空的,没有记录任何权限相关的信息 加用户,此时不进行任何认证还是可以做	。当admin.system.users一个 时任何操作(不管是否以—auth	·用户都设有时,即 (参数启动),直到在
AK建露检测	Redis 4x/5x 這個命令执行電電運用	admin.system.users中读	加一个用户。加速的核心方案是实现只有在 \$4.4.4.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1	admin.system.users中凉加电户之后,M	ongoD6890Ai£, BEE0889673	能生双。
	数道CA 這種代詞的行odsy編詞	请参考: https://help.ali	yun.com			
Stream Stream 2	Coremal範疇信息注意Oday應用	受影响资产				
选产指纹调查	Oracle WebLogic 远程命令执行0de/篇例	○ と号出漏	洞影响资产列表		未处理 > 編	、服务器の成名称
主动防御	Spring Cloud Config 服务运程任意文件读取局间(CVE-2014-3799)	· 侍友王忠文	·资产	说明	状态	1
网页防模改合	Confluence 远程命令统(行篇意篇调(CV5-2019-3199)	⊠ 8		100 10000	未修复	80E /
安全运营	MongoDB未提行調口令访问篇网			West of the second		2417
安全报告 New	Spring Boot Actuator 未成权访问远程代码执行震调		100000-0000	1000 C 100 C	*# #	82%E
安全大解	Jenkins 无条件远程代码执行地能编网	■ 32/E	2746 R0360206	每页显示 10 20	50 < 1-3	1 下一页

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。

臺開修复 系統屬則由計測: 2019年4月25日 15.1963 立即目前 快速转变属用前端 副						
Linux软件贏用 705 Windows系统氟制 20 Web-CMS贏制 6 啟用氟例 虚急贏用 4						
c		金郎 ~ 3	1993篇词名称 Q			
還興名称	披露时间 4	影响资产数	操作			
Webmin远程命令抗(万篇间(CVE-2019-15107)	2019年8月19日 23:07:50	已检测,智无风险	立即检测			
Apache Sor 远程命令约行推測(CVE-2019-0193)	2019年8月6日 20:00:11	检测中	立即检测			

・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。

識問修复	凝结漏洞扫	描时间: 2019年8月29日 1	5:19:03 立即	日描 快	速修复高河指南	局何苦理设置
Linux软件職詞 705 Windows系統職詞 20 Web-CMS職詞 6 应用職詞 20 成意識詞 4						
с			全部	^	查询漏洞名称	Q
通用名称	披露时间 4	影响资产数	全部	~		操作
Webmin运程命令执行篇同(CVE-2019-15107)	2019年8月19日 23:07:50	已检测,智无风险	存在风险			立即检测
Apache Solr 远缓命令执行漏洞(CVE-2019-0193)	2019年8月6日 20:00:11	已检测,暂无风险	JUNE			立即检测

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。

 第1. 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。

云安全中心	展現体質	©2000 5 个月前 MongoDB未授权弱口令访问漏洞					
93	Linux战化体赢用 705 Windows系统晚期 20 Web-CMS编用 6 应用最同0 应急编码 4	MongoDB数据库未授权 漏洞详情: https://he	7調口令访问震调,震调危害严重,可以导致数据 Ipaliyun.com	·库数描述重成设删除数素,从而 单击链接,查看漏洞更多	這成严重的生产事故。 多 <mark>信息。</mark>		
资产中心 New 99+	c	CVE	£	披露时间	2019年3月24日 09:00:54		
▼ 安全防范	識調案称	CVSS	Æ	危险等级	严重		
混涡修复 99+	Webminl匠程命令执行重调(CVE-2019-15107)	周 潤特征	66年2四				
	Apache Solv 回程命令执行魔响(CVE-2019-0193)	详情					
▼ 或粉检测	XStream < 1.4.11 远程代码执行推推赢用	満済危害 开启MongoDB服务后, 助作),而且可以远程。	如不添加任何参数,默认是没有权限验证的。登 方问数据库。	绿的用户可以通过默认猜口无需	王码对数据库进行任意操作(包括增、 蒙	1、改、童等高危	
安全告誓处理 49	Jackson 最新貶序列化漏除(CVE-2019-14361和CVE-2019-14439)	漏洞或因					
攻击分析	festjoon < 1.251 這程代時低行應用	安装完MongoD8服务后 MongoD8启动时添加了	武认有一个admin数据率,此时admin数据库是 一auth参数,如果没有在admin数据库中添加用	空的,没有记录任何权限相关的修 户,此时不进行任何认证还是可以	(息、当admin.system.users一个用户都设 以做任何操作(不管是否以一auth 参数回 のかりに、「ののののよう」。	2有时,即使 加,直到在	
AK过露检到	Redis 4x/5x 透檀命令执行高稳漏洞	admin.system.users中的	如一个用户,加减的核心方案是实现只有在adn	hin.system.users甲液加用甲乙酯,	MongoDB的认论、投机服务才能生效。		
▼ 調査明应 日本分析	取送CA 認知代時時(Floday)構成	· HorsexLix 代码的	◎复建议于和处理潮洞				
微步感動情报	Coremai和蓝色思想能day描词	受影响资产					
资产指纹调查	Crade WebLogic 运程命令执行Oday属詞	○ 坐 导出漏	洞影响资产列表		未处理 > 編入服务器(P或名称 Q	
▼ 主动防御	Spring Cloud Config 服务远程任意文件读取属两(CVE-2019-3799)	- 修用系物度	遗产	说明	秋志	操作事	
网页防要改合	Confluence 运程命令的行炮推漏周(CVE-2019-35%)	Z	410-078 (1-0-000 K	22 11 23	未修复	80E 2046	
▼ 安全巡营	MongaDB未接代源口令功间编制		10.00	1000 000000	±10.97	80.7 508	
安全接舌 New	Spring Boot Actuator 未接权访问远程代码执行篇例		100000-0000	10000		Sector (2040)	
安全大麻	Jenkins 无象体退退代码执行高度漏洞	1 10E	298 R.M.201	每页显示 10 3	80 50 く上一页 1	下一页 >	

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。



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
		\mathbf{x}	

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。

云安全中心	乘時撤送	系统漏洞扫	3描时间: 2019年7月	18日 10:15:13	立即扫描 快速修复漏洞描高 麗洞智	理論
总选	Linux统件兼阅 664 Windows系统规则 55 Web-CMS规则 11 应用规则 应急规则 2					
资产管理	C ±	未处理	× ≈ ×	Ф X	低 × × 按索漏洞名称	Q
▼ 安全防范	属同公告		影响资产		披露时间	操作
港河修复 99+	RHSA-2017;1916-中陸:glibc安全和BUG標編更新 (代码执行)		92		2019年7月18日 10:11:48	修复

3. 在漏洞管理设置页面,可执行以下操作:

漏洞管理设置			×
Linux软件漏洞:		共605台 (还有1台未开启)	管理
Windows系统漏洞:		共605台 (已全部开启)	管理
Web-CMS漏洞:		共605台 (还有1台未开启)	管理
应急漏洞:		共605台 (还有1台未开启)	管理
应用漏洞		扫描周期 ⑦ 一周 ~	
失效漏洞自动删除:	7天	\checkmark	
漏洞扫描等级:	✓ 高	☑ 中 ☑ 低	
漏洞白名单配置:			
漏洞公告			操作
2017-11-微软安全更	澵 (Windo	wws 2008R2 SP1) - KB4048960	移除
ecshop注入漏洞			移除
RHSA-2017:2478-重	要: httpd 安	全更新	移除
USN-3901-1: LinuxP	的核漏洞		移除
移除			

- ・ 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。

蕢 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。



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

- 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。
- 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。
- 8. 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

- 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

- 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

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等保合規检査 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

云安全中心		基线检查					策略管理				×	¢
98		 3 云安全中心 	已支持等级保护 20 基纯检查能力,请单击配置等保检查策略				- 1	每隔1天 在0~6点检测	63	32项	编辑 删除	1
资产中心 New	99+	基线检查策略			检查服务器数	检查项		每隔1天	677台	43项	编辑 删除	
▼ 安全防范		全部策略						在0~6点检测				
混同修复	99+	G Ŧ						每隔1天 在0~6抓检测	18	24项	编辑删除	
基状检查	34	等级	基线名称	基线检查项	风险项 / 影响服务器数		-	每隔1天 在0~6点检测	台	26项	编辑 删除	
CALL MARKED CO.		中盘	等保三级-CentOS Linux 7合规基线检查	15	13 / 224							
▼ 威胁检测 安全管整外理		中危	等保三级-Ubuntu合规基线检查	15	11 / 77		1000	每隔1天 在0~6点检测		26项	编辑 删除	
攻击分析		中危	等保二级-Ubuntu合规基纯检查	14	11 / 77			每隔1天 在0~6点检测	倍	26项	编辑 删除	ł
AK泄露检测		中盘	CIS标准-Ubuntu 16安全基线检查		10 64 12 / 52			每隔1天	4	0.078	1010 1010	I
▼ 调查响应		激放	阿里云标准-CentOS Linux 6安全基结检查	15	10 / 71			在0~6点检测	H	2044	2682 0012	I
日志分析		海龍	阿里云标准-CentOS Linux 7安全基线检查	15	10 / 224		-	每隔1天 在0~6点检测	台	26项	编辑 删除	l
微步威胁情报		中危	等保二级-CentOS Linux 7合规基线检查		10 / 224			每隔1天	(77)	0.078	1048 1046	I
资产指纹调查		中能	CIS标准-Windows Server 2008 R2安全墓线检查	274	9 118 32 / 32			在0~6点检测	0//15	2094	26424 02121	
▼ 主动防御 回司防護改合		中族	CIS标准-CentOS Linux 7安全器结检查	198	9 87 20 / 215			每隔1天 在0~6点检测	18	26项	9858 BID	4 第 1 4
▼ 安全运营		中危	CIS标准-CentOS Linux 6安全基线检查	197	9 83 20 /70		默认策略	每隔1天 在0~6点检测	678台	15项	编辑	1
安全报告 New							基本检查重要。	▼ 斎 ▼ 中 ▼ 年				I
应用市场												ļ
0E											ang Rin]

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。

策略管理				
4	每隔1天 在0~6点检测	台	32项	编辑 删除
	每隔1天 在0~6点检测	677台	43项	编辑 删除
	每隔1天 在0~6点检测	台	24项	编辑 删除
1000	每隔1天 在0~6点检测	台	26项	编辑 删除
	每隔1天 在0~6点检测	台	26项	编辑 删除
	每隔1天 在0~6点检测	台	26项	编辑 删除
	每隔1天 在0~6点检测	台	26项	编辑 删除
1000	每隔1天 在0~6点检测	台	26项	编辑 删除
1000	每隔1天 在0~6点检测	677台	26项	编辑 删除
	每隔1天 在0~6点检测	台	26项	编辑 删除
默认策略	每隔1天 在0~6点检测	678台	15项	编辑
基线检查等级: ▼	▲ 高 🔽 中 🔽 低			

· 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。

云安全中心	基线检查				快速检查基线问题 策略管理
总派	3 云安金中心已支持等级保护 2.0 基线检查能力, 遗单击配置等保检查算	18 <u>9</u>			
资产中心 New 99+	基线检查策略		检查服务器数 检查项	最近检查通过率	文印绘制
▼ 安全防范	默认策略 每隔1天在0点检测678台服务器	~	678 15	21%	进度详情
混河修复 99+	C ±			全部状态 >	全部横型 V 基线名称 Q
基线检查 34	##0 第44 2 95	部址於李箔	同院师 / 影倫認久將粉	其任论事 语心州	星に始春时间
云平台配置检查 15	NG-NA. BEDIKE-113*	BENERILE?*	PRE 2 0 2 0 000 MINA		-400112121-0_1140
w additional	高校 同里云标准-CentOS Linux 6安全基核检查	15	10 771	熟纸	2019年8月30日 05:02:57

·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。



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。

基线检查							快速核查基线问题	策略管理
1 云安全中心已支持等级保护 2.0 基线检查能力, 请单击配置等保检查策略								
漏送检查策略	_	检查服务器数	检查项	最近检查过	動过率		立即检测	
默认策略 每隔1天在0点检测678台服务器	<u>D</u>	678	15	21%			进度详情	
The second second second second					全部状态 > 全部	部英型 ~	基线名称	۹
等级保护2.0-三级合规检查	基线检查项	风险项 / 影响服务器数	τ	基线检查项分类			ş	最近检查时间
新たは101 (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (101) (10	15	10 / 71		系统			2019年8月3	10日 05:02:57
The second state of the se	15	10 / 224		系统			2019年8月3	10日 03:40:22

4. 单击立即检测。

基线检查				快速核查基线问题 策略管理
3 云安金中心已支持等级保护 2.0 基线检查能力, 请单主配置等保检查策略				
基廷检查等期 等级保护20-三级合规检查 時間3天在0点检測8726台影频器 ✓	检查服务器数 678	_{检查项} 16	最近检查通过率 12%	立即检测 进痰洋情

・执行立即检测后、检测概览区域将显示实时检测进度。

基线检查				快速核產基线问题 策略管理
⑧ 云安全中心已支持等级保护 2.0 整线检查能力, 请单击配置等保检查策略				
基线检查策略	检查服务器数	检查项	最近检查通过率	检测中 10%
等级保护2.0.二级合规检查 每隔3天在0点检测678台服务器 ✓	678	16	12%	进度洋橋

·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。

进度详情	\times
开始时间: 2019-08-30 10:56:00 结束时间	쾨: 2019-08-30 10:58:20
检测来源:手工检测 进度详情	青: 100% (成功578台, 失败100台, 进行中0台)
以下是检测失败的服务器列表, 查看解决方案。收起	
安装卸载001	A
-云助手安装卸载	1
10-01-01-01-01-01-01-01-01-01-01-01-01-0	
安装卸载001	•
	刷新进度详情 关闭

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。

云安全中心	基结检查				快速核查基线问题 策略管理
总派	● 云安金中心已支持等级保护 2.0 基线检查能力,请单击配置等保检查策略				
资产中心 New 99+	基线检查策略	检查服务器数	检查项	最近检查通过率	立即检测
▼ 安全防范	默认策略 每隔1天在0点绘测678台服务器	678	15	21%	进度详情
潤渇修复 99+	C ¥			全部状态 >> 全	部映型 V 基线名称 Q
基线检查 34	尊敬 基础名称	基线检查项 风险项 / 影响服务器	10 番紙社	查项分类	屬近检查时间
云平台配置检查 15 ▼ 成約公司	高名 阿里云标准-CentOS Linux 6安全基核检查	15 10 / 71	系统		2019年8月30日 05:02:57

- 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。

云安全中心		基线检查			等(f	R <mark>三级-CentOS Linux 7合规基线检查</mark> 25 Linux 7合规基线检查,对标中国等保2.0第三级等级保护基本要求部分检	查项目,仅供参考			×
93		 云安全中心E 	3支持等级保护 2.0 基线检查能力,清单击剧置等保检查策略							
资产中心 New S		基线检查策略			e	¥		资产名称		Q
• 安全防范		等级保护2.0	-三级合规检查 每隔3天在0点检测678台服务器	678		100,770	通过项	风险项		编作
温润修复 9		G F				A TO MARK & THE R. P. LEWIS	4	11	22	821Z
基线检查 3	34	带级	基线名称	基线检查项 风		AND CONTRACTOR CONTRACTOR	4	11	22	321E
云平台配置检查 * 威胁检测		中版	等保三级-CentOS Linux 7台烷基线检查	15		Contraction in the second	4	11	±#	验证
安全告誓处理 6		中危	等保二级-Ubuntu合规基纯检查	14				_		
攻击分析		中绘	總保三級-Ubuntu命現基結检查	15		Second Constants	4		<u>28</u>	REGE
AK泄露检测		中盘	等民二级-CentOS Linux 7合规基线检查	12		and from any figure at	7	8	22	验证
调查响应		中盘	等保三级-Windows 2008 R2合规基线检查	15		Strategy and strat	8	7	22 22	326E
日志分析		中島	等限二级-Windows 2008 R2合规器线检查	12		And and a second se	8			Rest.T.
资产推续调查		中危	瞭保三级-CentOS Linux 6合规基级检查	15		The second rear second		-		30.44
主动防御		中族	等保三级-Windows 2012 R2合现器结检查	15		The second se	8	7	27	824E
		中盘	等保三级-Debian Linux 8合规基线检查	15		and a second second	8	73		RNT
安全运营		中度	等保二级-Debian Linux 8合规基纯检查	14		a factor (1 of 1 of 1 of 1 of 1	-			- and
安全接管 New 应用市场						A REPORT OF A REPORT	8	7	±₩	验证
设置						酸还 每页显示 10 20	50 < L-	页 1 2 3 4 … 29	下一页	٤ >

· 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)。



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。

等保三级-CentO!	风险项	
	检查项	状态
	☐ 应对登录的用户进行身份标识和鉴别,身份标识具有唯一性,身份鉴别信息具有复杂度要求并定 期更换 身份鉴别	🗙 未通过 🛛 详情 验证 ;
	高 当对服务器进行远程管理时,应采取必要措施,防止鉴别信息在网络传输过程中被窃听 身份鉴别	🗙 未通过 🦳 详情 验证 /
	☐ 应具有登录失败处理功能,应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施↓身份鉴别	🗙 未通过 🦳 详情 验证 /
	高 应重命名或删除默认账户,修改默认账户的默认口令 访问控制	🗙 未通过 🦳 详情 验证 ;
	高 访问控制的粒度应达到主体为用户级或进程级,客体为文件、数据库表级 访问控制	🗙 未通过 🦳 详情 验证 ;
	高 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息 安全审计	🗙 未通过 🥂 详情 验证 /
•••	□ 応启用安全审计功能,审计覆盖到每个用户,对重要的用户行为和重要安全事件进行审计 安全 审计	🗙 未通过 🛛 详情 验证 វ
	高 应保护审计进程, 避免受到未预期的中断 安全审计	🗙 未通过 🦳 详情 验证 /
	高 应能发现可能存在的已知漏洞,并在经过充分测试评估后,及时修补漏洞 入侵防范	🗙 未通过 🦳 详情 验证 ;
	高 应能够检测到对重要节点进行入侵的行为,并在发生严重入侵事件时提供报警 入侵防范	🗙 未通过 🛛 详情 验证 ;
	忽略 取消忽略 每页显示 10 20 50	く 上一页 1 2 下一页

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。

等保三级-CentO: 风险项			
A-201 H 92-10-94		状态	操作
应对登录的用户进行身份标识和鉴别,身份标识具有唯一性,身份鉴别 X	予标识和鉴别,身份标识具有唯一性,身份鉴别信息具有复杂度要求并定	🗴 未通过	详情 验证 忽略
信息具有复杂度要求并定期更换 导份滥剂	时,应采取必要措施,防止^{坚则}信息在网络传输过程中被窃听 身份鉴	🗴 未通过	详情 验证 忽略
描述 检查以下内容: 1.检查量否存在空密闭账户; 2.身份衍识(UID)具有唯一性3.设置密码复杂度要求; 4.定期更换密码: 5. 质制密码重用。	8, 应配置并启用结束会活、限制非法登录次数和当登录连接超时自动退	🗴 未通过	洋情 验证 忽略
检查提示	9,修改默认账户的默认曰令 访问控制	🔀 未通过	详情 验证 忽略
	E体为用户级或进程级,客体为文件、数据库表级 访问控制	🔀 未通过	详情 验证 忽略
1、执行 查書空密码账户并处理:2、查 著 ,检查是否有重复UD的用户并清理3、编辑/ , , , 。 。 。 。 。 。 。 。 。 。 。 。 。 。 。 。	3期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息	🗴 未通过	详情 验证 忽略
7# 12	#计覆盖到每个用户,对重要的用户行为和重要安全事件进行审计 安全	🗴 未通过	详情 验证 忽略
ואן, אראראראראראראראראראראראראראראראראראראר	受到未预期的中断 安全审计	😢 未通过	详情 验证 忽略
操作时建议做好记录或备份	11漏洞,并在经过充分测试评估后,及时修补漏洞 入侵防范	😣 未通过	详情 验证 忽略
施定	我进行入侵的行为,并在发生严重入侵事件时提供报警 入侵防范	😣 未通过	详情 验证 忽略

送 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

说明:

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。

等保三级-CentOS	2 风险项	
	■ 检查项	状态
	高 应对登录的用户进行身份标识和鉴别,身份标识具有唯一性,身份鉴别信息具有复杂度要求并定 期更换 身份鉴别	★通过 详情 验证 单个执行"忽略"
	 高 当对服务器进行远程管理时,应采取必要措施,防止鉴别信息在网络传输过程中被窃听 身份鉴别 	🗙 未通过 🦳 详情 验证
	 高」 应具有登录失败处理功能, 应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退 出等相关措施 身份鉴别 	🗙 未通过 🦳 详情 验证
	高 应重命名或删除默认账户,修改默认账户的默认口令 访问控制	🗴 未通过 🦳 详情 验证
	高 访问控制的粒度应达到主体为用户级或进程级,客体为文件、数据库表级 访问控制	🗙 未通过 🧼 详情 验证
	 高 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息 安全审计 	🗙 未通过 🦳 洋情 验证
•••	高 应启用安全审计功能,审计覆盖到每个用户,对重要的用户行为和重要安全事件进行审计 安全 审计	🗴 未通过 🦳 详情 验证
	□ 高 应保护审计进程, 避免受到未预期的中断 安全审计	🗙 未通过 🧼 详情 验证
	☑ 高 应能发现可能存在的已知漏洞,并在经过充分测试评估后,及时修补漏洞 入侵防范	🗙 未通过 🦳 详情 验证
	☑ 高 应能够检测到对重要节点进行入侵的行为,并在发生严重入侵事件时提供报警 入侵防范	🔀 未通过 詳情 验证
	2 11/1 2% 哈 図略 取消忽略 每页显示 10 20 50	く 上一页 1 2 下-
_	-	

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。

风险	项		×
	检查项	状态	操作
	高 应关闭不需要的系统服务、默认共享和高危端口 入侵防范	✓ 已通过	详情 验证
	高 应遵循最小安装的原则,仅安装需要的组件和应用程序 入侵防范	✔ 已通过	详情 验证
	高 应对登录的用户进行身份标识和鉴别,身份标识具有唯一性,身份鉴别信息具有复杂度要求并定 期更换 身份鉴别	已忽略 单个执行"取消忽略"	取消忽略
	高 当对服务器进行远程管理时,应采取必要措施,防止鉴别信息在网络传输过程中被窃听 身份鉴别	! 已忽略	取消忽略
	高 应具有登录失败处理功能,应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退 出等相关措施↓身份鉴别	! 已忽略	取消忽略
	2 取消忽略 批量执行"取消忽略" 每页显示 10 20 50	く 上一页 1 2	下—页 >

- 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。



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	\checkmark
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	\checkmark
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	\checkmark

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	\checkmark
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	\checkmark
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	\checkmark
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	\checkmark
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	\checkmark
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	\checkmark
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	V
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。	\checkmark	\checkmark
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。	\checkmark	\checkmark
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。		V
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。	\checkmark	\checkmark
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。	\checkmark	\checkmark
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。	\checkmark	√
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。	\checkmark	\checkmark
SLB-健康状态	监控告警	检测SLB后端服务器是否可用。	\checkmark	\checkmark
SLB-证书过期检	监控告警	检测SLB的可用证书是否已过期。	\checkmark	\checkmark
OSS-Bucket权限 设置	数据安全	检测OSS Bucket权限是否设置成了私 有。	\checkmark	\checkmark
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。	\checkmark	\checkmark
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。		\checkmark
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。	\checkmark	\checkmark
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。	\checkmark	\checkmark
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。	√	1
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。	\checkmark	√
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。	\checkmark	\checkmark

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。

云平台配置检查					快速了解云平台配置检测能力检测设置
风脸项	影响资产数	未启用检查项	已處用检查项	最近检查时间	立即绘测
15 💶 💿 💷	129	0	44	2019年8月29日 16:10:06	

b. 设置云产品配置项的检测周期和检测时间。

检测设置		×
检测周期:	星 X 星 X 星 X ✓ 星 X 星 X 星 X ✓	
检测时间:	06:00 - 12:00 ~	
	确定取消	ij

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。


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。



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。

・ 査看检测详情

- 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。



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。