# 查看漏洞控制面板

Cisco Secure Workload 可识别并在**漏洞 (Vulnerabilities)** 页面上显示所有工作负载的已知常见漏洞和风险 (CVE) 列表。使用显示的评分和 CVE 的严重性，您可以将精力集中在最需要关注的最严重漏洞和工作负载上。选择评分系统和范围，根据严重性和其他属性详细信息查看 CVE。

Cisco Secure Workload 中使用的不同评分系统包括：

- 通用漏洞评分系统 (CVSS)：CVSS 是 CVE 严重性的定性衡量标准，级别从低到严重。评分可帮助您确定最关键严重性的响应优先级。CVSS V3 是 CVSS 评分机制的最新版本。

**表 *1:* 评分系统和相应属性**

| 评分系统 | 属性 |
| --- | --- |
| CVSS V3 | • 具有严重性的 CVE 评分<br>• 攻击复杂性<br>• 攻击媒介<br>• 可用性影响<br>• 基本严重性<br>• 保密性影响<br>• 完整性影响<br>• 所需权限<br>• 范围<br>• 用户交互 |

| 评分系统 | 属性 |
| --- | --- |
| CVSS V2 | • 具有严重性的 CVE 评分<br>• 访问复杂性<br>• 访问向量<br>• 身份验证<br>• 可用性影响<br>• 保密性影响<br>• 完整性影响<br>• 严重性 |

该控制面板突出显示了所选范围内的漏洞分布情况，并按不同属性显示漏洞，例如，漏洞利用的复杂性、能否通过网络来利用漏洞，或者攻击者是否需要本地访问工作负载。此外，统计信息还能过滤出可被远程利用且利用复杂性最低的漏洞。

通过从 NIST、Microsoft 和 Oracle 等常见来源检索最新的 CVE 详细信息，Cisco Secure Workload 中的 CVE 威胁数据库每 24 小时更新一次。如果 Cisco Secure Workload 集群处于气隙环境中，则必须从 https://updates.tetrationcloud.com 下载 CVE 威胁数据包并上传到 Cisco Secure Workload。

通过使用工作负载中已知 CVE 的评分和所需属性，您可以：

- 创建资产过滤器。请参阅资产过滤器。
- 配置微分段策略以阻止来自受影响工作负载的外部通信，并将虚拟修补规则发布到Cisco Secure Firewall Management Center。


- 漏洞控制面板, on page 2
- CVE 选项卡, on page 4
- “软件包”(Packages) 选项卡, on page 4
- “工作负载”(Workloads) 选项卡, on page 5
- “Pod”选项卡, on page 7


# 漏洞控制面板

要查看“漏洞”(Vulnerabilities) 页面，请从导航窗格中选择**调查 (Investigate)** > **漏洞 (Vulnerabilities)**。系统将显示使用不同评分系统识别出的漏洞。图表和构件会根据评分系统显示漏洞数量、相关风险级别和属性，以确定需要立即关注的工作负载和需要立即打补丁以降低风险的软件包。

***Figure 1:*** *“漏洞”(Vulnerabilities)* 页面

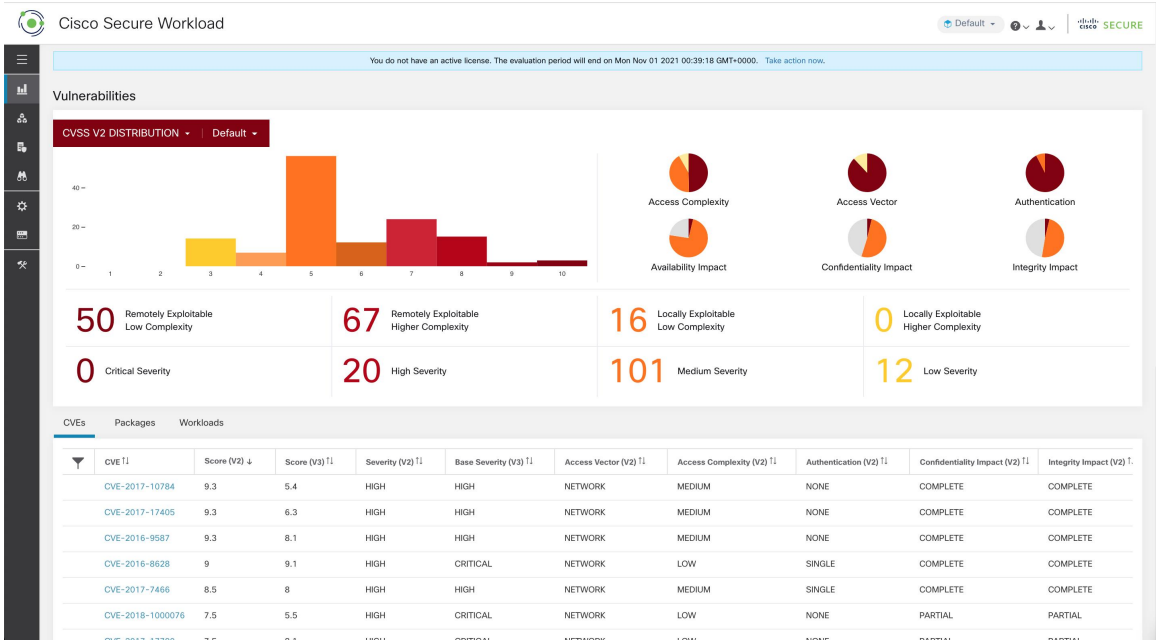
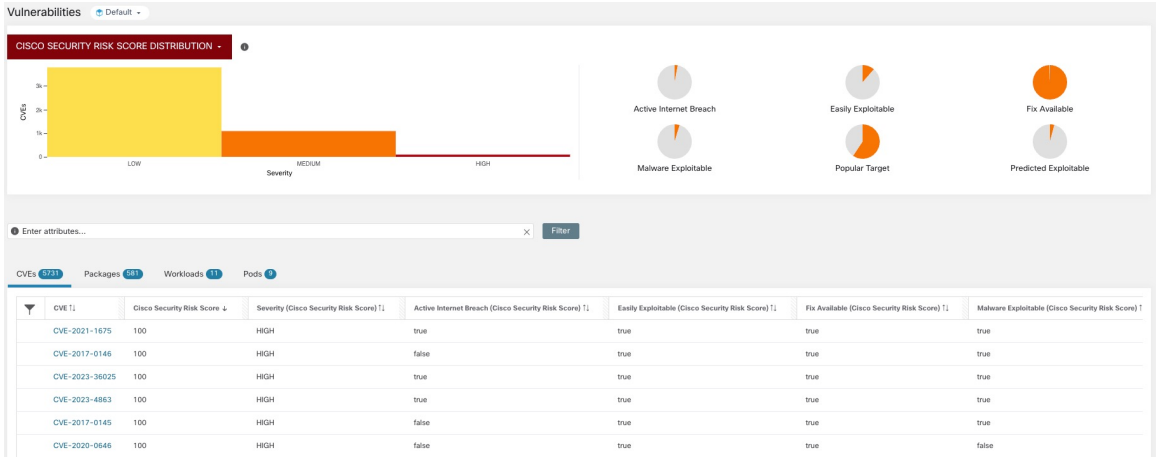



***Figure 2:*** *“漏洞”(Vulnerabilities)* 页面




以下选项卡根据图形或构件的选定部分进行过滤：

- **CVE** 选项卡会突出显示所选范围内需要注意的漏洞。
- **软件包 (Packages)** 选项卡列出了必须修补的软件包。
- **工作负载 (Workloads)** 选项卡列出所选范围内受影响的工作负载。
- **Pod** 选项卡列出所选范围内受影响的 Kubernetes Pod。

有关详细信息，请点击选项卡中所需的行。例如，点击“软件包”(Packages)选项卡中的一行，以查看安装了软件包或版本的工作负载以及该软件包的关联漏洞。可使用下载链接将显示的列表下载为 JSON 或 CSV 文件。

# CVE 选项卡

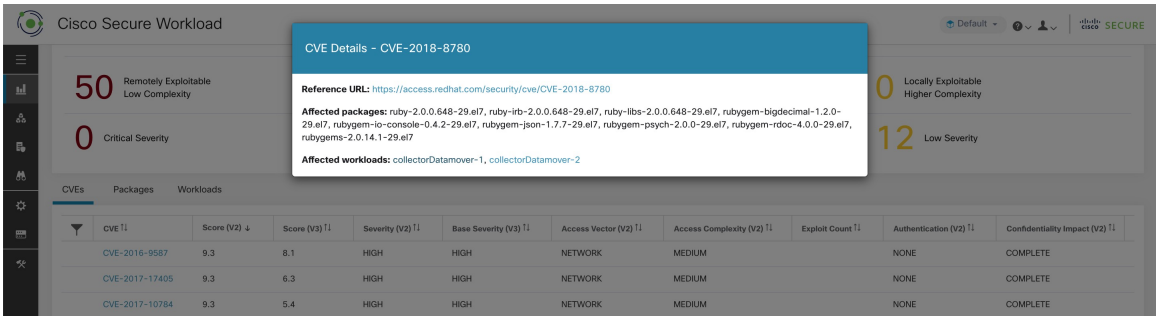
根据评分系统和所选范围，CVEs 选项卡会列出在工作负载上发现的漏洞。对于每个 CVE，除了基本影响指标外，还会显示基于 Cisco Secure Workload 威胁智能的漏洞攻击信息：

- 漏洞利用计数：组织中过去一年被利用的 CVE 次数。
- 上次被利用时间：上次发现 CVE 在组织中被 Cisco Secure Workload 的威胁智能利用的时间。

图表和饼图可用于根据严重程度或评分系统的要求属性来过滤 CVE。例如，如果点击任何评分系统中的“关键”严重性栏，表格将仅显示包含严重 CVE 的工作负载、软件包和 Pod。

点击“CVE”选项卡下所需的行，以获取有关该漏洞和受影响工作负载的更多详细信息。

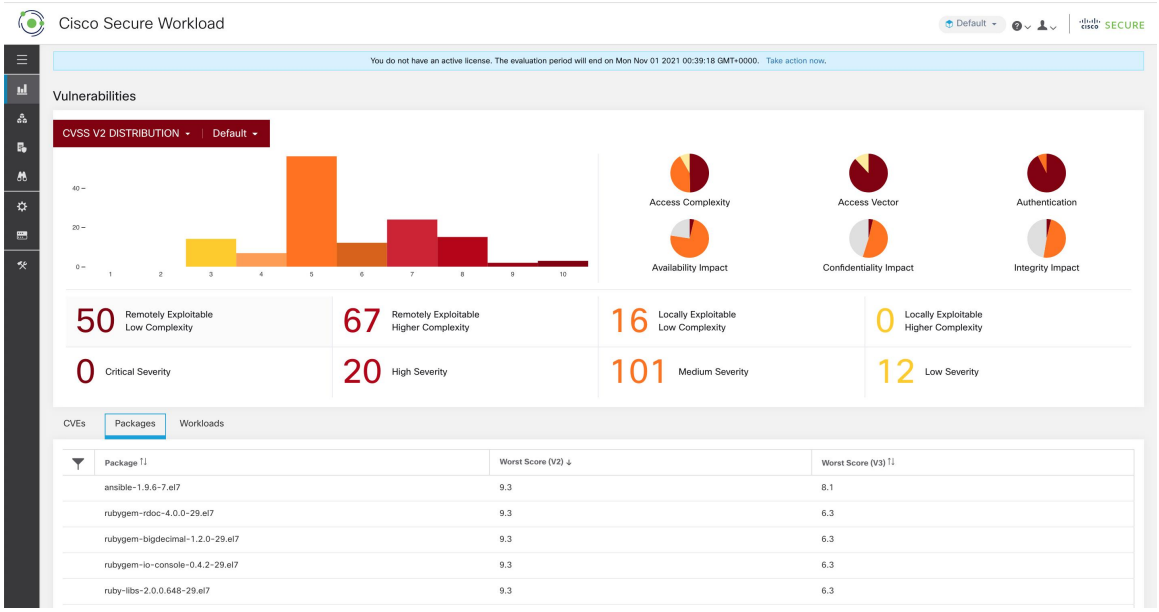
***Figure 3: CVE* 的详细信息**




# “软件包”(Packages) 选项卡

“软件包”(Packages) 选项卡列出了受影响的软件包，必须升级这些软件包才能减少攻击面。

***Figure 4:*** *“软件包”(Packages)* 选项卡列出指定范围内易受攻击的软件



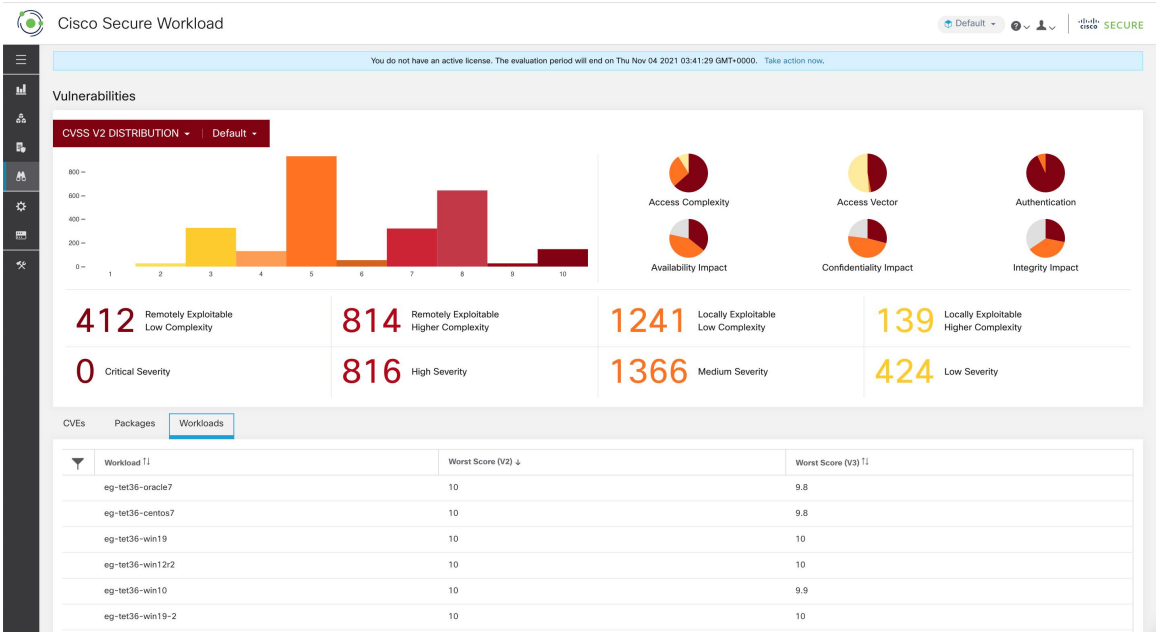

点击“软件包”(Packages)选项卡下所需的行，以获取有关受影响软件包、包含该软件包的工作负载以及软件包中已识别的 CVE 的更多详细信息。

***Figure 5:*** *软件包的漏洞和受影响工作负载的详细信息*


# “工作负载”(Workloads) 选项卡

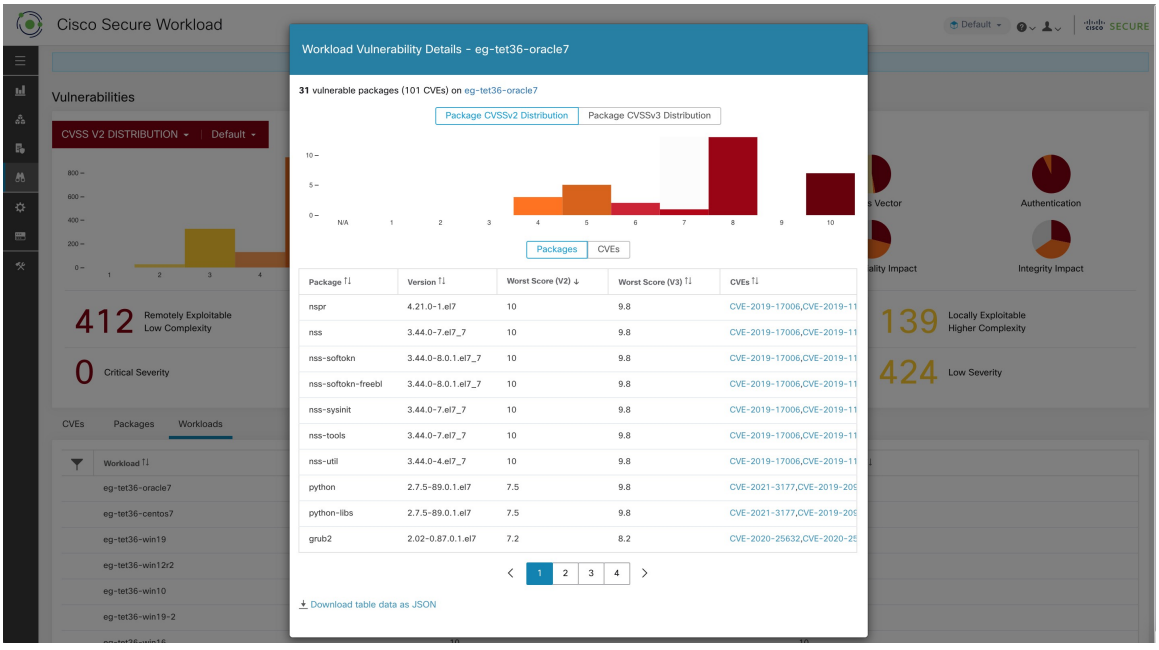
“工作负载”(Workloads) 选项卡列出了需要立即关注软件更新或补丁的工作负载。

***Figure 6:*** *“工作负载”(Workloads)选项卡列出指定范围内易受攻击的工作负载*




点击“工作负载”(Workloads)选项卡下所需的行，以获取有关所选工作负载中存在的易受攻击的软件包的更多详细信息。要查看工作负载配置文件，请点击对话框标题旁边的工作负载名称。

***Figure 7:*** *受影响工作负载中的漏洞详细信息*



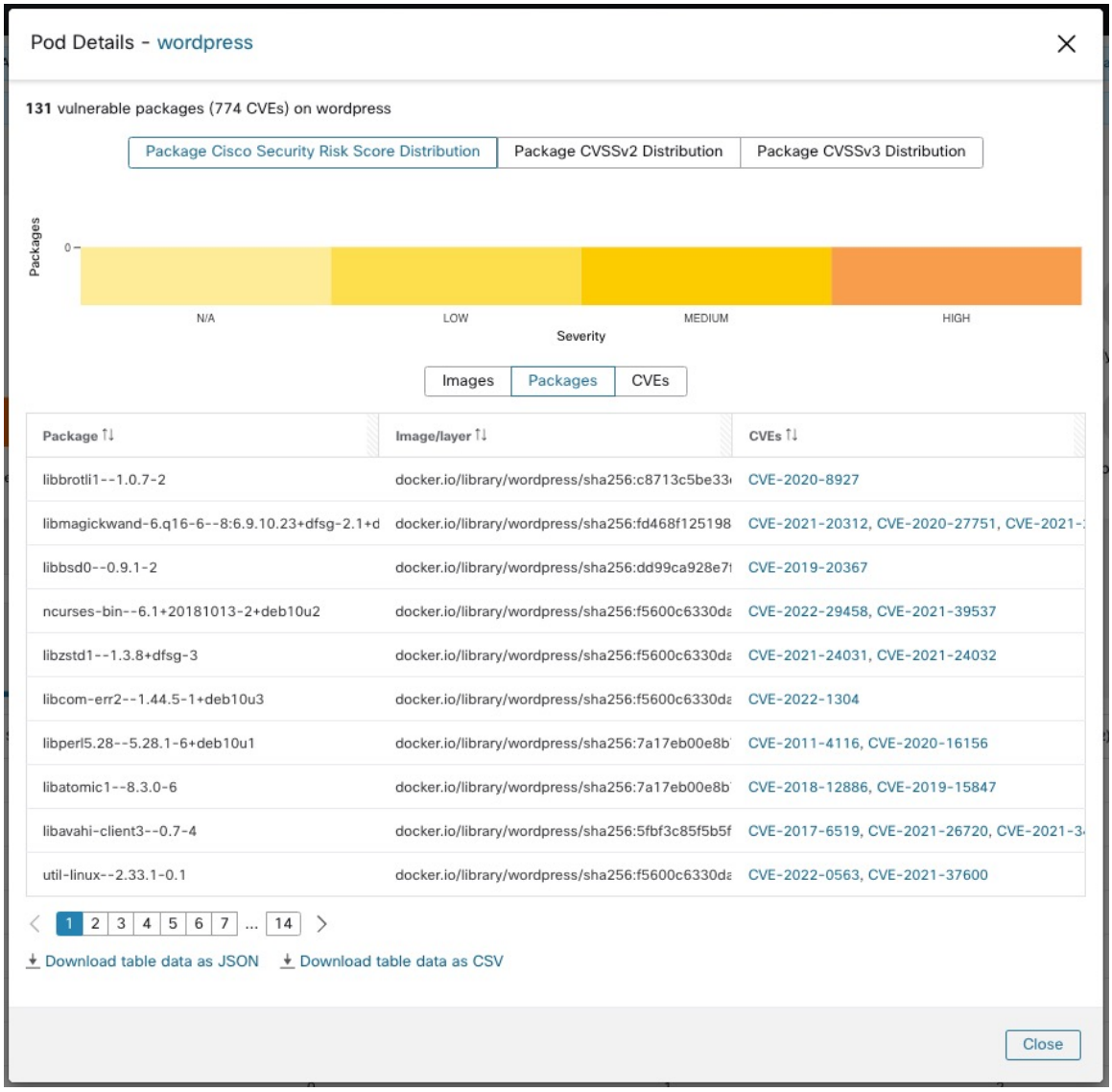

您可以选择工作负载，并以 CSV 文件的形式下载影响工作负载的漏洞摘要。

# “Pod”选项卡

“Pod”选项卡列出了在软件更新或补丁方面需要立即关注的 Kubernetes Pod。

点击“Pod”选项卡下所需的行，以获取有关受影响的 Kubernetes Pod、软件包、映像和已识别的 CVE 的更多详细信息。

***Figure 8: Kubernetes Pod* 中的 *CVE* 和受影响的软件包**



当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。