



红帽产品勘误 [RHSA-2023:6264 - Security Advisory](#)

## RHSA-2023:6264 - Security Advisory

发布：2023-11-02 已更新：2023-11-02

概述

更新的软件包

### 概述

Important: insights-client security update

### 类型/严重性

Security Advisory: Important

#### Red Hat Lightspeed patch analysis

识别并修复受此公告影响的系统。

[查看受影响的系统](#)

### 标题

An update for insights-client is now available for Red Hat Enterprise Linux 8.2 Advanced Update Support, Red Hat Enterprise Linux 8.2 Telecommunications Update Service, and Red Hat Enterprise Linux 8.2 Update Services for SAP Solutions.

Red Hat Product Security has rated this update as having a security impact of Important. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) in the References section.

## 描述

Red Hat Insights is a service that provides analysis of registered Red Hat-based systems. The insights-client package can gather the required data (such as installed packages, running services, or software configurations) to proactively identify threats to security, performance, and stability across your environment.

Security Fix(es):

- insights-client: unsafe handling of temporary files and directories (CVE-2023-3972)

For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.

## 解决方案


For details on how to apply this update, which includes the changes described in this advisory, refer to:

<https://access.redhat.com/articles/11258> 


## 受影响的产品

- Red Hat Enterprise Linux Server - AUS 8.2 x86\_64
- Red Hat Enterprise Linux Server - TUS 8.2 x86\_64
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.2 ppc64le
- Red Hat Enterprise Linux for x86\_64 - Update Services for SAP Solutions 8.2 x86\_64

## 修复

- [BZ - 2227027](#)  - CVE-2023-3972 insights-client: unsafe handling of temporary files and directories

## CVE

- [CVE-2023-3972](#) 

## 参考

- <https://access.redhat.com/security/updates/classification/#important> 

---

Red Hat 安全团队联络方式为 [secalert@redhat.com](mailto:secalert@redhat.com)。更多联络细节请参考 <https://access.redhat.com/security/team/contact/>。



Quick Links



Help



Site Info



Related Sites



Loading



[About Red Hat](#)

[Jobs](#)

[Events](#)

[Locations](#)

[Contact Red Hat](#)

[Red Hat Blog](#)

[Inclusion at Red Hat](#)

[Cool Stuff Store](#)

[Red Hat Summit](#)

© 2026 Red Hat

[Privacy statement](#)

[Terms of use](#)

All policies and guidelines

Digital accessibility

Cookie preferences