

[Red Hat Product Errata](#)    [RHSA-2023:6283 - Security Advisory](#)

# RHSA-2023:6283 - Security Advisory

Issued: 2023-11-02    Updated: 2023-11-02

[Overview](#)[Updated Packages](#)

## Synopsis

Important: insights-client security update

## Type/Severity

Security Advisory: Important

### Red Hat Lightspeed patch analysis

Identify and remediate systems affected by this advisory.

[View affected systems](#) 

## Topic

An update for insights-client is now available for Red Hat Enterprise Linux 8.

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.

## Description

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.

## Solution

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

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

## Affected Products

- Red Hat Enterprise Linux for x86\_64 8 x86\_64
- Red Hat Enterprise Linux for x86\_64 - Extended Update Support Extension 8.8 x86\_64
- Red Hat Enterprise Linux for x86\_64 - Extended Update Support 8.8 x86\_64
- Red Hat Enterprise Linux for IBM z Systems 8 s390x
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 8.8 s390x
- Red Hat Enterprise Linux for Power, little endian 8 ppc64le
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 8.8 ppc64le
- Red Hat Enterprise Linux Server - TUS 8.8 x86\_64
- Red Hat Enterprise Linux for ARM 64 8 aarch64
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 8.8 aarch64
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.8 ppc64le
- Red Hat Enterprise Linux for x86\_64 - Update Services for SAP Solutions 8.8 x86\_64
- Red Hat Enterprise Linux for x86\_64 - Extended Life Cycle 8.10 x86\_64
- Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 8.10 aarch64
- Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 8.10 ppc64le
- Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 8.10 s390x

## Fixes

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

## CVEs

- [CVE-2023-3972](#)

## References

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

---

The Red Hat security contact is [secalert@redhat.com](mailto:secalert@redhat.com). More contact details at <https://access.redhat.com/security/team/contact/>.



The image shows a dark-themed navigation bar for the Red Hat website. On the left is the Red Hat logo, which consists of a red fedora hat icon and the text "Red Hat" in white. To the right of the logo are four social media icons: LinkedIn, YouTube, Facebook, and X. Below the logo and icons is a vertical list of navigation items, each with a white downward-pointing chevron icon to its right: "Quick Links", "Help", "Site Info", and "Related Sites".

 Partial system outage



[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](#)