

This bug is in the 'Embargoed' Data Category and access to this data must be restricted as per the [Data Reuse Policy](#).



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

**Keywords:** Security

**Reported:** 2023-07-27 13:18 UTC by TEJ RATHI

**Status:** NEW

**Modified:** 2023-11-08 10:59 UTC [\(History\)](#)

**Alias:** CVE-2023-3972

**CC List:** 11 users [\(show\)](#)

**Product:** Security Response

**Fixed In Version:** insights-client 3.2.2

**Component:** vulnerability

**Clone Of:**

**Version:** unspecified

**Environment:**

**Hardware:** All

**Last Closed:**

**OS:** Linux

**Embargoed:** Yes

**Priority:** high

**Severity:** high

**Target Milestone:** ---

**Assignee:** Nobody

**QA Contact:**

**Docs Contact:**

**URL:**

**Whiteboard:**

**Depends On:** 2229674 2229675  
 2229676 2229677  
 2229678 2229679  
 2229680 2229681  
 2229682 2229683

**Blocks:** 2222203

**TreeView+** [depends on](#) / [blocked](#)

<b>Attachments</b>	<a href="#">(Terms of Use)</a>
--------------------	--------------------------------

#### Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	<a href="#">RHSA-2023:6264</a>	0	None	None	None	2023-11-02 09:22:06 UTC
Red Hat	<a href="#">RHSA-2023:6282</a>	0	None	None	None	2023-11-02

Product Errata						12:31:52 UTC
Red Hat Product Errata	<a href="#">RHSA-2023:6283</a>	0	None	None	None	2023-11-02 12:38:23 UTC
Red Hat Product Errata	<a href="#">RHSA-2023:6284</a>	0	None	None	None	2023-11-02 12:36:53 UTC
Red Hat Product Errata	<a href="#">RHSA-2023:6795</a>	0	None	None	None	2023-11-08 08:28:06 UTC
Red Hat Product Errata	<a href="#">RHSA-2023:6796</a>	0	None	None	None	2023-11-08 08:21:12 UTC
Red Hat Product Errata	<a href="#">RHSA-2023:6798</a>	0	None	None	None	2023-11-08 08:34:31 UTC
Red Hat Product Errata	<a href="#">RHSA-2023:6811</a>	0	None	None	None	2023-11-08 10:59:55 UTC

TEJ RATHI 2023-07-27 13:18:19 UTC

[Description](#)

The unsafe handling of temporary files and directories in insights-client. An unprivileged user can corrupt any files owned by root.

[🔒 https://bugzilla.redhat.com/show\\_bug.cgi?id=2222156](https://bugzilla.redhat.com/show_bug.cgi?id=2222156)

Sandipan Roy 2023-11-01 11:01:41 UTC

[Comment 5](#)

Making the issue Public.

Sandipan Roy 2023-11-01 11:01:57 UTC

[Comment 6](#)

<https://github.com/RedHatInsights/insights-core/pull/3878>

errata-xmlrpc 2023-11-02 09:22:05 UTC

[Comment 9](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 8.2 Advanced Update Support  
Red Hat Enterprise Linux 8.2 Update Services for SAP  
Solutions  
Red Hat Enterprise Linux 8.2 Telecommunications Update  
Service

Via RHSA-2023:6264 <https://access.redhat.com/errata/RHSA-2023:6264>

errata-xmlrpc 2023-11-02 12:31:51 UTC

[Comment 10](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9

Via RHSA-2023:6282 <https://access.redhat.com/errata/RHSA-2023:6282>

errata-xmlrpc 2023-11-02 12:36:51 UTC

[Comment 11](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 8.6 Extended Update Support

Via RHSA-2023:6284 <https://access.redhat.com/errata/RHSA-2023:6284>

errata-xmlrpc 2023-11-02 12:38:21 UTC

[Comment 12](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 8

Via RHSA-2023:6283 <https://access.redhat.com/errata/RHSA-2023:6283>

errata-xmlrpc 2023-11-08 08:21:11 UTC

[Comment 13](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9.0 Extended Update Support

Via RHSA-2023:6796 <https://access.redhat.com/errata/RHSA-2023:6796>

[2023:6796](#)

errata-xmlrpc 2023-11-08 08:28:05 UTC

[Comment 14](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 7

Via RHSA-2023:6795 <https://access.redhat.com/errata/RHSA-2023:6795>

errata-xmlrpc 2023-11-08 08:34:30 UTC

[Comment 15](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 8.4 Advanced Mission Critical Update Support

Red Hat Enterprise Linux 8.4 Update Services for SAP Solutions

Red Hat Enterprise Linux 8.4 Telecommunications Update Service

Via RHSA-2023:6798 <https://access.redhat.com/errata/RHSA-2023:6798>

errata-xmlrpc 2023-11-08 10:59:53 UTC

[Comment 16](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 8.1 Update Services for SAP Solutions

Via RHSA-2023:6811 <https://access.redhat.com/errata/RHSA-2023:6811>

---

**Note**

You need to [log in](#) before you can comment on or make changes to this bug.

