



CVE-2022-38130

Published on: Not Yet Published

Last Modified on: 08/15/2022 04:11:00 PM UTC

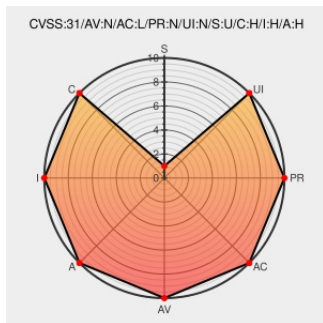
CVE-2022-38130

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Sensor Management Server](#) from [Keysight](#) contain the following vulnerability:

The

`com.keysight.tentacle.config.ResourceManager.smsRestoreDatabaseZip()` method is used to restore the HSQLDB database used in SMS. It takes the path of the zipped database file as the single parameter. An unauthenticated, remote attacker can specify an UNC path for the database file (i.e., `\\<attacker-host>\sms\<attacker-db.zip>`), effectively controlling the content of the database to be restored.

CVE-2022-38130 has been assigned by vulnreport@tenable.com to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVE References

Description	Tags	Link
Keysight Technologies Sensor Management Server Multiple RCE Vulnerabilities - Research Advisory Tenable®	www.tenable.com text/html	MISC www.tenable.com/security/research/tra-2022-28

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to

comment@cve.report.


There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Keysight	Sensor Management Server	2.4.0	All	All	All
cpe:2.3:a:keysight:sensor_management_server:2.4.0:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVereport	CVE-2022-38130 : The com.keysight.tentacle.config.ResourceManager.smsRestoreDatabaseZip method is used to restore... twitter.com/i/web/status/1...	2022-08-10 20:29:23

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2022   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)